

History of changes

Version	Date	Description of changes	Revised by
0.1	31/01/2018	Task 1.4 duration changed from M3-M15 to M3-M12; Deliverable 1.3 and Milestone 3 submission deadline moved from M15 to M12; Task 1.5 duration changed from M1-M28 to M1-M30; Data Management Plan and Standardization and IPR report has been separated; Data Management Plan deliverable (D7.5) moved to M3 from M30; T2.2 leader changed to INOV; T6.5 leader changed to ATOS; in T2.2 3PMs switched from ATOS to INOV; in T6.5 3PMs switched from INOV to ATOS; BRZ's PMs redistributed as follows: WP1: 0,5PM, WP4: 3PM, WP6: 0,25PM, WP7: 0,25PM; Security Advisory Board added to Task 5.1 and Section 6; Workpackage 8 (Ethics requirements) added; GANTT chart updated;	István Böröcz (VUB), Paul De Hert (VUB), Carmela Occhipinti (CEL), Tomas Piatrik (QMUL)
0.2	31/01/2018	Released version submitted to EU	István Böröcz (VUB)
0.3	05/02/2018	Means of verification to Milestones added; minor style corrections	István Böröcz (VUB), Carmela Occhipinti (CEL), Tomas Piatrik (QMUL)
0.4	05/02/2018	Release version submitted to EU	István Böröcz (VUB)



Table of Contents

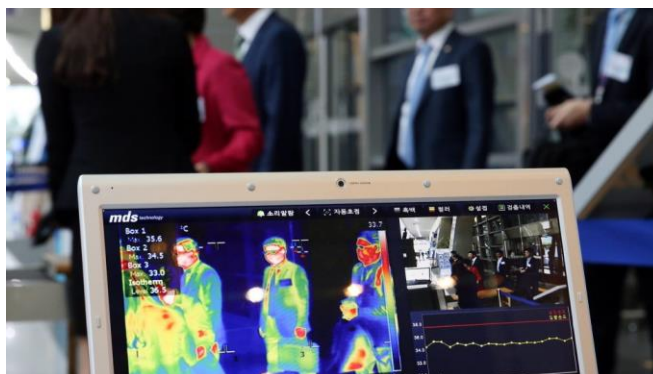
1. EXCELLENCE	4
1.1 OBJECTIVES	5
1.2 RELATION TO THE WORK PROGRAMME.....	8
1.3 CONCEPT AND METHODOLOGY	9
1.3.1 <i>Overall Approach</i>	10
1.3.2 <i>PERSONA orchestration framework for assessment of no-gate crossing point technologies</i>	12
1.3.3 <i>PERSONA use cases and field deployments</i>	15
1.3.4 <i>National/International research & innovation activities</i>	16
1.3.5 <i>Gender Analysis</i>	17
1.4 AMBITION	18
1.4.1 <i>Privacy and data protection aspects of border crossing</i>	18
1.4.2 <i>Ethical aspects of border crossing</i>	20
1.4.3 <i>Regulatory aspects of border crossing</i>	21
1.4.4 <i>Social aspects of border crossing</i>	23
2 IMPACT	25
2.1 EXPECTED IMPACTS	27
2.1.1 <i>Societal impact</i>	31
2.1.2 <i>Barriers and necessary conditions</i>	32
2.2 MEASURES TO MAXIMISE IMPACT.....	32
2.2.1 <i>Dissemination plan</i>	32
2.2.2 <i>Communication Activities</i>	33
2.2.3 <i>Linking to other projects & public outreach</i>	34
2.2.4 <i>Data Management Plan</i>	35
2.2.5 <i>Exploitation of Project Results</i>	35
2.2.6 <i>Research Data and Intellectual Property Rights (IPR) Management</i>	38
2.2.7 <i>Contribution to Standards and International Initiatives</i>	39
3 IMPLEMENTATION	41
3.1 WORK PLAN — WORK PACKAGES, DELIVERABLES AND MILESTONES.....	41
3.2 MANAGEMENT STRUCTURE AND PROCEDURES	42
3.2.1 <i>Governance</i>	43
3.2.2 <i>Research and Innovation Management</i>	45
3.2.3 <i>Decision making and conflict management</i>	45
3.2.4 <i>Reporting and communication</i>	45
3.2.5 <i>Quality monitoring</i>	46
3.2.6 <i>Risk Management</i>	46
3.3 CONSORTIUM AS A WHOLE.....	46
3.3.1 <i>Complementarity of participants</i>	46
3.4 RESOURCES TO BE COMMITTED	49
3.4.1 <i>Personnel Effort</i>	49
3.4.2 <i>Labour and other direct costs</i>	50
3.4.3 <i>Subcontracting</i>	50
3.4.4 <i>Resource Mobilisation</i>	50
3.4.5 <i>Detailed Resources Breakdown</i>	50
4 MEMBERS OF THE CONSORTIUM	52
4.1 PARTICIPANTS (APPLICANTS).....	52



4.1.1	<i>Vrije Universiteit Brussel</i>	52
4.1.2	<i>Peace Research Institute Oslo (PRIO)</i>	56
4.1.3	<i>Cyberethics Lab</i>	58
4.1.4	<i>Atos</i>	60
4.1.5	<i>INOV INESC INOVAÇÃO</i>	62
4.1.6	<i>Queen Mary University of London (QMUL)</i>	66
4.1.7	<i>Swedish Police Authority, National Forensic Centre (SPA)</i>	70
4.1.8	<i>Bundesrechenzentrum – Federal Computing Centre</i>	71
4.1.9	<i>Ministry of Interior of the Republic of Serbia (SMOI)</i>	75
4.1.10	<i>Ministry of Public Security – Israel National Police (MOPS)</i>	77
4.2	THIRD PARTIES INVOLVED IN THE PROJECT (INCLUDING USE OF THIRD PARTY RESOURCES).....	80
5	ETHICS AND SECURITY	82
5.1	ETHICS.....	82
5.1.1	<i>Privacy and data protection</i>	82
5.1.2	<i>General data protection principles</i>	82
5.1.3	<i>Relevant legal regulations</i>	83
5.1.4	<i>The European Union’s data protection framework</i>	84
5.1.5	<i>Protection of privacy and personal data in police and judicial cooperation in Europe</i>	84
5.1.6	<i>The revision of the EU data protection framework</i>	85
5.1.7	<i>PERSONA Ethical Management Strategies</i>	86
5.1.8	<i>Security measures for storage and handling of data</i>	88
5.1.9	<i>Protection of Ethnic and other sensitive Information of Participants</i>	88
5.1.10	<i>Informed Consent</i>	88
5.1.11	<i>Ethical standards for research</i>	90
5.1.12	<i>Ethics Self-Assessment</i>	90
5.2	SOCIETAL IMPACT	93
6	SECURITY	95

1. Excellence

The increasing number of travellers crossing European borders is putting a mounting pressure on the everyday handling of border checks. The European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, state that there are over 500 million intra-EU arrivals per year and the number is rapidly growing with every year. On one side, border control authorities have to



process a higher number of checks in an increasingly reduced amount of time to avoid congestion or cope with limited resources. The experience of both European and third country travellers is deteriorating due to the extra time they have to spend at the border checkpoints. Such a continuous need calls for flexible, automated and scalable “no-gate” border security solutions. On the other side, the intensive use of technologies bears the risk to invading people’s privacy, and the societal and political acceptance of technologies for contactless border security solutions is required prior to their implementation.

Proactive thinking is not entirely new for most of the actors both in the public and private sphere, however, mapping, analysing and evaluating future occurrences is an ambitious task, even with access to vast amount of information and to high-end processing power. Due to legal requirements and market demands, professional or self-regulatory obligations, internal risk-management and different forms of risk or impact assessments (IA) are performed on a regular basis. For example, in the recent years the reliance on risk management to protect privacy has noticeably increased, although without a comprehensive, widely accepted model. To successfully identify and treat potentially adverse consequences of deployed border solutions, a solid framework for the assessment method is essential. The relevance of this ambition lies in the difficulty of establishing an adequate impact assessment method: as from a methodological point of view, *“there is no ‘silver bullet’ method for carrying out impact assessments. What matters is the choice of an appropriate assessment method allowing for the best understanding and treatment of possible consequences of the envisaged initiative”*.¹

Methods developed to perform impact assessment of border security solutions also needs to generate information useful for decision-makers to take informed decisions about future technology deployments, and for industry to design products that preserve privacy and other societal concerns such as ethics or societal acceptance. The importance of the inclusion of the various relevant legal and societal concerns when assessing the impacts of a technology on an individual is crucial as surveillance and other border controlling technologies can affect e.g. not only the right to the protection of personal data, but other rights as well (e.g. the right to privacy), furthermore ethical, societal, economic and political impacts.

A pivotal element of the PERSONA project is ***to design and establish effective methods for and carry out an impact assessment able to appropriately assess the effects of new border-controlling technologies and to ensure that these solutions meet the requirements and expectations of both governments, LEAS and border crossing individuals.***

¹ d.pia.lab Policy Brief No. 1/2017

1.1 Objectives

The ultimate objective of PERSONA is to develop a unified and tailored impact assessment method and carry out comprehensive assessments of the acceptability of wide range of contactless crossing point technologies, **taking into account human behaviour, gender, legal frameworks, privacy concerns, societal issues and potential risks of discrimination**. The established method for assessment will **provide important information for decision-makers in form of potential risks, mitigation measures and guidelines**, in order to drive the innovation and deployment of future solutions by industry and border authorities.

To fulfil this mission, PERSONA will achieve the following specific objectives and Key Performance Indicators (KPIs):

Obj 1: To carry out privacy, ethical, regulatory, and social assessment of the acceptability and impacts of no-gate crossing point solutions

PERSONA will perform a throughout impact assessment of no-gate crossing point technologies and solutions on border crossing individuals, addressing the relevant privacy, ethical, regulatory and societal concerns. Consequently, based on the assessment results, PERSONA will provide solutions and guidelines for stakeholders and decision-makers on how to design such solutions or treat the undesired effects adequately. By addressing all the relevant concerns of the deployment of no-gate border-crossing technologies, its effects on the observed will be adequately defined. The importance of the inclusion of the various relevant legal and societal concerns when assessing the impacts of a technology on an individual is crucial as surveillance and other border controlling technologies can affect e.g. not only the right to the protection of personal data, but other rights as well (e.g. the right to privacy), furthermore ethical, societal, economic and political impacts. PERSONA will address all characteristics of the event or technology under assessment, its type and complexity thereof, type and number of individuals concerned, and the project will also be responsive to geographical and cultural differences.

KPIs

- The range of over 30 latest and new-generation no-gate crossing point solutions will be assessed.
- Over 200 individuals will take part in thorough assessment of selected no-gate solutions

Obj 2: To develop and establish a unified, tailored-down impact assessment method for no-gate crossing point solutions

Beside assessing the effectiveness and perception of border crossing technologies, PERSONA is in a strong position to develop a unified method for performing assessments on the impacts of these technologies. To achieve this objective, the research will be comprised by the elaboration on and the evaluation of the relevant privacy, ethical, regulatory and societal concerns, affected by border crossing technologies and their respective method of assessment, such as privacy impact assessments, data protection impact assessments, ethical impact assessments and social impact assessments. The ultimate goal of the PERSONA is to establish a unified impact assessment method, focusing *inter alia* on a concrete list of steps and processes to be taken, the designation of the impact assessment team, timeline, resources, tips and tricks, dos and don'ts, and resulting in clear and concrete guidelines and best practises. To ensure the effectiveness, universality, and flexibility of the assessment methodology and processes, PERSONA partners will engage in the development process with a large group of carefully selected key decision makers, border authorities, leading service providers and other stakeholders as part of the established Advisory Board and Network of

stakeholders. The developed method will be tested and shaped during carefully designed field technology deployments, and throughout close collaboration with BES-15 actions and other relevant EU projects.

KPIs	<ul style="list-style-type: none"> • All current European privacy, ethical, regulatory and social regulations, focusing on individual rights and needs when being screened by border technologies, will be evaluated and addressed by the PERSONA impact assessment • The group of over 20 carefully selected key decision makers, service providers, social experts and stakeholders will take part in defining and shaping the PERSONA assessment method
------	--

Obj 3: To analyse, select and setup the latest technologies enabling no-gate crossing point solutions for assessment

The PERSONA technical partners (ATOS, INOV and QMUL) are bringing together a wide range of expertise and solutions for the border security domain. These partners will bring to the project over 15 of the latest technologies and solutions for the border screening, ranging from complete commercial mobile solutions to technologies dealing with data analytics, biometrics, encryption and decision making in border control. Furthermore, to significantly broaden the impact and scope of the project, PERSONA will go far beyond the technologies brought by its internal partners. The projects technical partners will make a thorough study and analysis of existing and new-generation technologies and solutions developed by EU projects, with special focus on BES-15 actions. The most relevant and highly effective solutions developed in these projects will be carefully selected and close synergies will be built between PERSONA and relevant projects. The PERSONA's goal is to cover all currently used commercial solutions, latest research and innovation solutions and next-generation prototypes in areas of video analytics, 3D scanning, abnormal activity detectors, object or vehicle detectors, soft biometrics, emotion or stress detectors, multimodal information processing and fusion, data protection and data management.

KPIs	<ul style="list-style-type: none"> • The set of over 30 of the latest technologies and solutions for no-gate border crossing will be analysed and setup for assessment • Over 15 technologies and solutions to be assessed in close collaboration with relevant projects and BES-15 actions
------	---

Obj 4: To liaison with BES-15 actions and other related projects

The synergy and close cooperation with relevant EU security projects and initiatives developing innovative and state-of-the-art solutions for no-gate crossing points is at the heart of the PERSONA's strategy. PERSONA's technical partners will exploit their direct involvement in current or past projects developing targeted security solutions, including ATOS (ABC4EU), INOV (ASGARD, FLYSEC, ROCSAFE) and QMUL (LASIE, SAFESHORE). On top of that, PERSONA will select the most successful EU projects through close study of developed technologies, but the biggest emphasis will be put on actions resulting from SEC-15-BES-2017 call (Risk-based screening at border crossing). A special non-disclosure agreement will be designed by VUB and PRIO in order to allow safe and effective cooperation with selected projects and perform the impact assessment on their developed technologies. As an outcome, PERSONA will deliver the results from the assessment to these projects for their internal reporting and extended evaluations.

KPIs	<ul style="list-style-type: none"> • Cooperation with over 8 selected projects for the assessment of the technologies built in these projects
------	--



Obj 5: To develop the orchestration framework with a tailored interface and tools to facilitate the assessment of the technologies

PERSONA is envisioned to assess the latest and next generation solutions and sensors for no-gate crossing point technologies and as such, should interact with the environment of field agent deployments. To enable this action, PERSONA will develop the orchestration frameworks comprising of advanced user interfaces and protocols to enable efficient and flawless integration, interaction and assessment of a wide range of technologies brought by both, project partners and companies from relevant projects. The orchestration framework will offer a seamless ecosystem for assessment of diverse technologies through the instantiation of operational and communication protocols. The orchestration methodology will include the construction of events encountered by assessed individuals when engaged in a number of checks by set of several types of no-gate solutions deployed in a defined sequence. This dedicated framework will be designed for maximum performance, accessibility and stability to fully support the large-scale testing and assessment of provided technology and solutions.

KPIs	<ul style="list-style-type: none">• The orchestration framework will enable to connect, test and assess over 20 diverse scanners, sensors and no-gate crossing point solutions
------	--

Obj 6: To communicate the best practises and guidelines with decision makers and key stakeholders

The outcomes of the PERSONA's comprehensive acceptance assessment will be persistently communicated with stakeholders and decision-makers in order to inform on important insight about the guidelines, best practises and identified risks, from the different points of view of those actors who can change the system and those who can be affected by it. By ensuring direct and effective engagement with stakeholders, PERSONA will pass on important information that will give the existing and new generation no-gate crossing point solutions a competitive advantage in terms of increased transparency, awareness, acceptability and trust. To ensure that the set of guidelines and mitigation measures are communicated timely and effectively with right group of decision makers, PERSONA will establish a dedicated Advisory Board and Network of Stakeholders, consisting of technology experts and leading service providers, border authorities of the key European countries, end-users of the BES-15 and other relevant projects, and experts in social, ethics and privacy issues. To enable effective communication and exchange of important information, PERSONA will use appropriate tools such as online communication and sharing platforms, wiki, webinars and teleconference system.

KPIs	<ul style="list-style-type: none">• PERSONA will be communicating its findings with over 60 selected key stakeholders and decision makers• 3 dedicated workshops will be organised to serve as an important tool for engagement with key stakeholders
------	--

Obj 7: To produce and publish a white-label, freely available and reusable textbook on guidelines for developing and operating no-gate crossing point solutions

The result of the PERSONA research will be a concrete, ready-made, fully-customisable, white-label and freely available and reusable textbook to be provided to its main group of addressees, meaning organizations which will develop crossing point solutions and border authorities which will use border crossing technologies. This textbook will be designed, drafted, tested, validated and disseminated in cooperation with their intended users, throughout the project's term. In this way,



PERSONA will result in relevant and timely impact assessment method, that will address decision-makers' immediate need for such method. Valuable human and financial resources that would otherwise be required to develop such method will be freed by PERSONA, so as to be used in actual work. The textbook will be printed in 5000 copies and distributed among partners and stakeholders. The published textbook will be a lasting legacy of the PERSONA project and have a true impact on the evolution of border security solutions and acceptance of such solutions by travellers and individuals crossing borders.

KPIs	<ul style="list-style-type: none">• The PERSONA textbook will be made available online in digital form as well as printed and distributed by end of the project• The PERSONA textbook will be disseminated via range of media channels, including social pages, built up mailing lists, relevant conferences and workshops, and EC online tools
------	--

1.2 Relation to the Work Programme

The topic of the call addressed by PERSONA is SEC-18-BES-2017 as shown in the following table:

<p>Work Programme: The assessment of the acceptability of such (combinations of) technologies and systems by citizens (who need to remain in control of personal data) and practitioners is needed, that takes account of human behaviour, gender, legal frameworks, societal issues, and possible risk of discrimination.</p>
<p>PERSONA Action:</p> <p>Building on long term expertise of VUB, PRIO and CEL partners, PERSONA will analyse the existing assessment methodologies and establish a tailored-down method for the assessment of the acceptability of border crossing technologies by individuals crossing the border, either at the airport or via land crossing points. Using this method, and the specially designed orchestration framework, PERSONA will assess the impacts of no-gate crossing point technologies on the relevant privacy, ethical, regulatory and societal concerns, and provide solutions for how to treat the undesired effects adequately. The scope of concerns in PERSONA can be justified through the wide range of impacts caused by such technologies. Establishing a unified impact assessment method which covers the assessment of the impacts on multiple concerns and share the knowledge through free, relevant, and immediately usable guidelines, PERSONA contributes directly to the effective implementation and application of technology impact assessments as per the call's priority.</p>
<p>Work Programme: Methods developed to perform such assessments need also to generate information useful for decision makers to take informed decisions about future technology deployments, and for industry to design products that preserve privacy.</p>
<p>PERSONA Action:</p> <p>PERSONA will develop a unified method for performing an impact assessment on no-gate crossing point solutions, in order to generate information and methodology useful for decision-makers and assisting them in taking informed decisions regarding the development and deployment of border crossing technologies. To reach the widest range of authorities and developers, the final outcome of the research will be materialized as a textbook, suitable for organizations developing or authorities deploying border crossing technologies to carry out an impact assessment. PERSONA will thus result in:</p>

- (a) Identifying the benefits and drawbacks of a wide range of steps to be taken during an Impact Assessment;
- (b) Exploring the positive and negative effects of the process on various categories of stakeholders
- (c) Addressing these findings through the development of an appropriate method for border authorities;
- (d) Saving-up decision-makers' financial and human resources while developing guidelines necessary for the adequate use of impact assessments;
- (e) Improving the harmonisation of impact assessment methods across the EU, through the use of uniform materials for carrying out an impact assessment;
- (f) Achieving effective implementation and application of the relevant legislative frameworks.

1.3 Concept and Methodology

Emerging technologies can be both beneficial and detrimental to the society at large and to the individuals concerned. Technologies employed at border checks – equally for the purposes of increasing border security like for smoothing the border crossing experience – are no exception. At least two interests compete in such a situation: the promised benefits of a new technology in terms of speeding border controls and the protection against the abuse of such a technology.² Since both interests are legitimate, there is a critical need to find a thin red line between these two.

The PERSONA consortium is very aware of such a need, and the challenges that it implies. To that end, the PERSONA project adopts a pro-active and self-reflexive ethical approach, based on an increasing wealth of research that highlights the potential of impact assessment methodologies to serve as a means for fair balancing.³

Therefore, the PERSONA consortium will develop a tailored method and framework for **assessing the impacts of the carefully selected current and new generation no-gate crossing point technologies** – in an integrated way – against **ethical, regulatory and social acceptance issues**. This framework will be subsequently used to assess **both the research conducted and the prototype under development** and – eventually – to feed the functional and non-functional requirements. Furthermore, the consortium will establish three internal oversight bodies and will apply a policy for the participation in the research. (A detailed approach is discussed in Section 1.3.1.)

Given the complexity of the issues at stake, the scope of such impact assessment cannot be of a singular nature. Experience has shown that in the context of emerging technologies, the sole focus of an impact assessment on “the classic criteria”, i.e. privacy and personal data, does not exhaust all societal concerns these technologies might raise. These usually concern intertwined matters such as state security, economic well-being, ethics or – perhaps one of the most pertinent – abusive surveillance.⁴ For this reason, the PERSONA ethical approach will be also informed by novel research

² Cf. e.g. Kindt, Els, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis*. Law, Springer, 2013; Ball, Kirstie, Kevin D Haggerty, and David Lyon, *Routledge Handbook of Surveillance Studies*. Taylor & Francis, 2012; Gutwirth, Serge, “Biometrics between Opacity and Transparency,” *Annali dell’Istituto Superiore Di Sanita* 43 (2007), pp. 61–65.

³ Kloza, Dariusz, Niels van Dijk, and Paul De Hert, “Assessing the European Approach to Privacy and Data Protection in Smart Grids. Lessons for Emerging Technologies,” In *Smart Grid Security. Innovative Solutions for a Modernized Grid*, ed. Florian Skopik and Paul Smith, pp. 11–47. Elsevier, 2015.

⁴ Raab, Charles D., and David Wright, “Surveillance: Extending the Limits of Privacy Impact Assessment.” In *Privacy Impact Assessment*, ed. David Wright and Paul De Hert, pp. 363–83. Springer, 2012.



about social acceptance of border check technologies and current border security practices at the external EU frontiers. Finally, the consortium will **provide ethical, legal and societal recommendations** concerning the integration of emerging technologies for border security into EU and national policies.

1.3.1 Overall Approach

The PERSONA Impact Assessment methodology and framework intends to be broader than what art. 35 GDPR⁵, the article that makes impact assessment an obligation for data controllers when the processing of personal data constitutes a high risk to the rights and freedoms of the natural person, requires: the project's IA mobilises not only data protection law but other relevant societal concerns such as privacy, ethics and social acceptance issues. The assessment is an iterative process, as it does not have a clear ending point. The first iteration of the process will be conducted in the first year of the project. It is critical to ensure that the recommendations (as the outcome of the IA) are sufficiently implemented. The implementation of the recommendations will be monitored, and documented in periodic reviews-reports. This ensures that the impact assessment remains transparent. The assessment is publicly accessible, thus the public at large can be informed about the existence of an assessment process, its terms of reference, the method and its progress. The main elements of an impact assessment can be defined, although, as there is no one-size-fits-all model for impact assessments, it can be modified whenever necessary.

1. Threshold analysis - The primary aim of an impact assessment is to assess potential impacts of an application (or a project) in terms of adherence to the relevant societal concerns. A preliminary threshold analysis (initial assessment) should be carried out in order to determine whether an impact assessment is necessary and if yes, what are the relevant societal concerns affected by the proposed activity. An assessor should be able to seek non-binding advice from external experts in case of doubt, without disclosing confidential information. There are several reasons why an IA process needs to be initiated. These can include *inter alia* a requirement for admissibility; acknowledgement by an organisation that a proposal has broad and significant implications that should be subjected to an impact assessment; public concerns; etc. In synthesis, this stage includes:

- Pre-assessment of the need to conduct an impact assessment
- Selection of criteria, e.g., on which the pre-assessment is conducted, e.g., impacts on rights and freedoms, impacts on social norms, impacts on market, motivations and timing, legal basis and public concerns

2. Initiation of the assessment – As part of the initiation of the assessment the decision-maker should determine the roles and responsibilities of the team which conducts the impact assessment. The designated team, along with those who set the direction of the application or technology development (i.e. internal stakeholders), should determine the appropriate scale of an impact assessment. The role of this step within the context is to outline in broad terms the benchmarks related to the societal concerns that will be relevant during the assessment. If, after the threshold analysis, the risks or impacts are deemed to be not significant, then the scale of the IA could be limited. If the risks or impacts are significant, then an IA should be more detailed. The size or budget for a project is not a useful indicator of its likely impacts. The continuity of the IA should be ensured.

The second phase within the initiation stage is the determination of the grounds against which the impact assessment is to be conducted. The role of this step within the aforementioned context is to

⁵ <http://www.privacy-regulation.eu/en/35.htm>



outline in broad terms the legal and ethical principles that will apply to the initiative. These requirements will be used to create an “impact framework” which will apply the requirements outlined to the initiative. These requirements will be clarified with the internal stakeholders. In synthesis, this stage includes:

- Designation of the IA team
- Defining the resources needed
- Setting the determining grounds

3. Identification, characterisation and description of the system – The decision-maker might not be an expert in the various requirements, therefore to conduct the assessment the stakeholders need to cooperate with experts from various fields, for instance, law, ethics or engineering. Strong cooperation, in terms of effective and regular communication between the parties, and exchange of information between the parties has a pivotal role. To achieve strong cooperation, on the one hand, the project partners shall describe extensively the details and functioning of the project; on the other hand, the IA team shall describe the reasoning behind the entire assessment, including its goals, length, stages, intermediate and final results, liabilities and possible consequences.

Issues can also arise from the different goals and professional language the parties use. The meaning and importance of the various requirements might be self-evident for the IA team, but entirely confusing for other project partners, and vice-versa. The parties need patience, openness and the intention to understand the point of view of the other party. There are numerous, developed tools for the parties which help to understand the main goals of the procedure, e.g. charts or questionnaires. This stage includes:

- The use cases
- System information
- Description of primary and supporting assets of the system

4. Analysis of the impacts – As anticipated above, initiatives (events), interpreted either as risks or impacts, are the core elements and subjects of an impact assessment. The rationale behind the assessment is mitigating or avoiding adverse consequences prior to their occurrence. The analysis focuses on the understanding of the identified risk/impact, by analysing it. The result of the analysis should be compared with a classification system (i.e. benchmark) in order to evaluate the risk/impact. The evaluation will enable to single out the elements which need some form of treatment in order to minimize or avoid the adverse consequences. In synthesis, this stage includes:

- Identification of relevant risks
- Analysis of feared events
- Evaluation of feared events

5. Compliance check - If the risk-classification system is based on legal provisions, the assessment of the impacts on the relevant societal concern (e.g. on the right to the protection of personal data, regulated by the GDPR) will become a legal compliance check. The goal of compliance check is to define, whether the proposed activity complies with legal provisions.

6. Contingency plan - When the risks/impacts have been clarified and evaluated the impact assessment identifies appropriate and effective responses and mitigation techniques, such as means to avoid/transfer/mitigate/accept risks or impacts. During the selection of the appropriate treatment measure, the decision-maker takes into equal consideration all the previously defined requirements. At this stage, the decision-maker must make clear on which risks/impacts related to the relevant societal concerns are residual and accepted/acceptable. Finally, during this step, the decision-maker must bear in mind that, failing to address the identified risks or impacts may result in social, economic or reputational damages to himself/herself. This stage includes:

- Assessment of implemented and planned controls
- Identification and recommendation of controls
- Risk treatment and resolution
- Residual risks and risk acceptance

7. Monitoring and review - Review and/or audits are critical to ensure that the IA is, first, carried out properly and, second, that its recommendations are sufficiently implemented. Review and/or audits are indispensable, as project leaders might initially state that they accept and would implement the suggested mitigation measures, but in reality, they might fail to implement them. Thus, the implementation of the contingency plan is monitored and periodic reviews should be conducted. In case the system changes in a significant way as to affect the impact on the relevant societal concerns, depending on the magnitude of the changes, the IA is revised (wholly or partially) and carried out again. This stage includes:

- Periodic monitoring and review
- Flexibility of IA in case scenarios change

8. Stakeholder consultation – The main goal of the engagement of stakeholders is to provide insight about the identified and analysed risks, from the different points of view of those actors who can change the system and those who can be affected by it. If the impact assessment is conducted by a single viewpoint, risks and their impacts might be overlooked. A consultation with stakeholders can ameliorate the analysis of the risks, impacts and mitigating measures by collaborating with internal and external stakeholders. If the stakeholder engagement is conducted properly, it will give the application a competitive advantage in terms of increased transparency, trust, such as by providing assurance of the outcome of the impact assessment; better collection of risk/impact information; increased mutual understanding among decision-makers and stakeholders; better communication of the results of the assessment; improved awareness; etc. It must be borne in mind that public participation (which is part of the external stakeholders' involvement) echoes in the wording of art. 41 of the Charter of the Fundamental Rights of the European Union, which states that “the right of every person to be heard, before any individual measure which would affect him or her adversely is taken”. Therefore, stakeholder engagement is not only a suggestion but could also be construed as a legal requirement. In synthesis, this stage includes:

- Identification of internal and external stakeholders
- Organisation of three dedicated workshops
- Consultation
- Incorporation of the consultation in the assessment report

To ensure wide spread dissemination of the resulted guidelines, PERSONA will publish a white-label textbook, which will represent long term impact and legacy of the PERSONA work.

1.3.2 PERSONA orchestration framework for assessment of no-gate crossing point technologies

The main objective of the PERSONA orchestration framework is to enable assessment of wide range of no-gate solutions using dedicated user interface and communication protocols. The framework will not only simulate sensors, subsystems or airport systems, but simulate situations, run test scenarios, run stories and replay exactly the same story when needed, thus enabling to simulate and then physically assess acceptance of no-gate crossing point technologies, without the need to have a full real operational system. The PERSONA orchestration framework will be a simulator of simulators that can run synchronized or independent, and have the following capabilities:

- Emulate security sensors, i.e. for the PERSONA backend, one simulator should have the same behaviour as of a real sensor (sensors can be any device);



- Input files, for definition of events in specific time;
- Several sensor simulators can run at same time;
- Tool to test the PERSONA applications, that allows:
 - To repeat specific scenarios (stories);
 - Reproduce complex scenarios (e.g. full Proof of Concept (POC) scenarios);
 - Simulate dangerous situations (example: explosive detection alarms);
- Support PERSONA's operational training
- Simulator output events are logged with time stamp

Three main groups of components will exist within the PERSONA orchestration framework:

- PERSONA Control Module
This module will control (as options) all simulators in a synchronized manner. Functionalities identified to control the simulation include: Repeat, Start, Stop, Pause, Resume and Exit, as in figure below (Figure 1) - an example of a possible GUI Manager interface. To support quick simulation start, all scenarios will be preloaded and pre-processed in cache.

Optionally, it will be possible to run a script to control the simulation (e.g. Excel file) and pause the simulator in a specific time. The user can also have access to nested pause events. Dashboard information, status information (example presented in **Hiba! A hivatkozási forrás nem található.**), a status semaphore (RED the simulator is running/busy and GREEN the simulator is free), are also to be included.

- GUI Management Interface

Two types of simulators are identified, Pull – query based (e.g. RFID reader) and Push – time driven based (SIU – Simulator Interface Unit). The PERSONA orchestration framework is composed by the PERSONA Control Module and two types of Simulators, Push time-driven based (SIU – Simulator Interface Unit) and Pull type-query based (e.g. RFID reader). An overview of the GUI Management Interface (User Interface) is presented in Figure 2, configured with three sensors with Pull support and three Push (RFID) sensors.

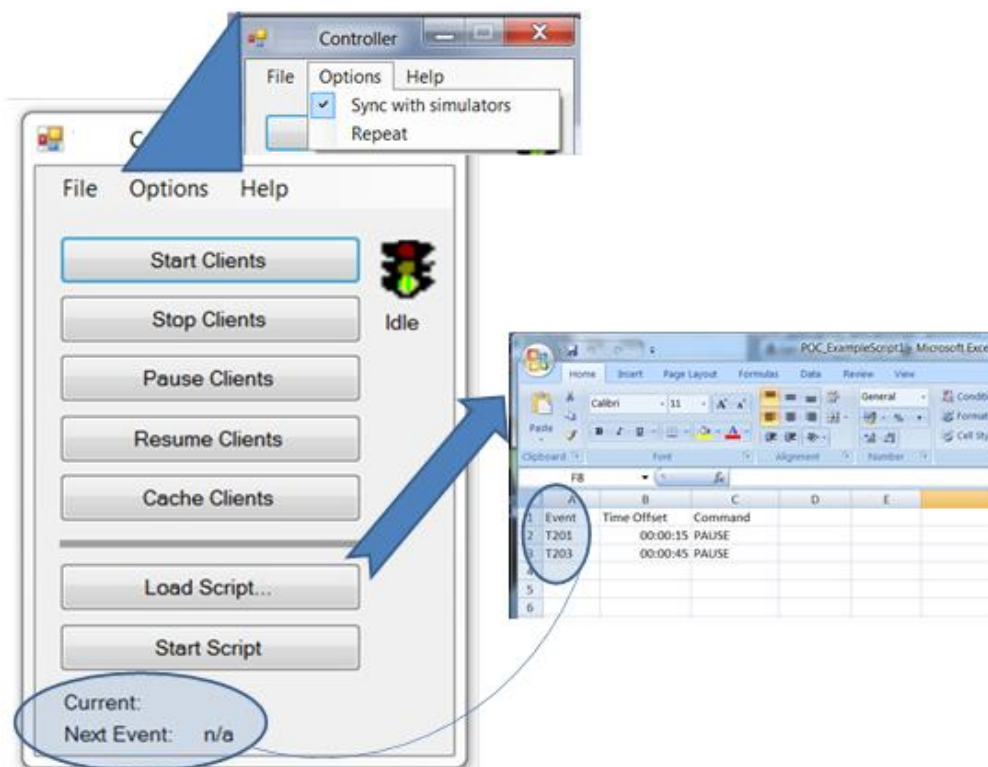


Figure 1 – PERSONA orchestration framework – Control Module

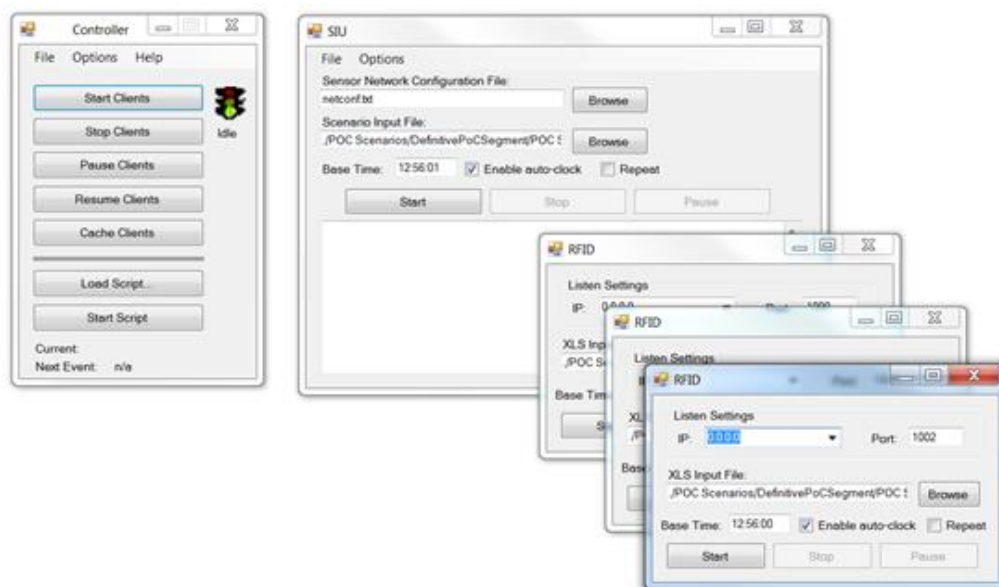


Figure 2 – The PERSONA orchestration framework – Overview of GUI Management Interface

Each simulator (Push or Pull type) has associated commands to control the simulator, used when synchronized mode is not available. Note each Simulator Interface Unit can simulate different types of sensors and several at same time, different protocols will be supported (socket, http, Web Service, Rabbit MQ Channel published) and with different behaviours (time-based, event-based).

- GUI USER interface (design for specific sensor): There are simulators that require an interface with the user in real time, as example, an overview of a simulator configured as

“communication interception system”: the user has the same functionalities as a real system, the interface allows the real management of each request received from different sources. After user authentication, inputting the username and password that was provided to him, user will have access to the Interception State List interface, seen (**Hiba! A hivatkozási forrás nem található..1**), makes the Evaluation of interception requests, and decides how the information is presented or accessed to other menus:

- Log Activity, the user access to Metadata and audio file associated to each interception
- Edit Phone Default, Update or Delete information associated with a phone number, the user can associate simulation scripts to a phone number and allows the user to pre-define the simulator procedure when an interception request is received (e.g. auto-accepted, auto-rejected or manual accept/reject).

Below is the list of the sensors, scanners, data analytics modules and decision systems brought together by PERSONA partners ATOS, INOV and QMUL available for assessment:

- Motion detection, based on Passive InfraRed (PIR) or ultra-sonic;
- Chemical and weather sensor;
- Inertial sensor, sensor based on gyroscope or/and accelerometer;
- Water Poisoning, chemical sensor;
- GPS, mounted on vehicle (e.g. taxi, bus, truck) with I/O interface (e.g. ignition ON/OFF, door status);
- Body & Luggage Scanner;
- Unmanned Ground Vehicle (UGV) with chemical sensor on board;
- Face Recognition sensor;
- Access control;
- IMSI Catcher, detect IMSI, IMEI and other information of an mobile-phone;
- Video Management System, system Camera that detect: Abandon Object, Trip Wire, Loitering and LPR;
- Vehicle & Cargo Scanning, Objects and Counts and Material and Percentages;
- Flight data, Season and Resource info, airport operation management system;
- Surface Movement Guidance and Control System(SMGCS) Radar, Object Localization i.e. Surface movement radar (SMR).
- DecidEasy: Decision Support System
- No-gate crossing point mobile system
- National Facilitation Programme
- Person trackers based on distinctive region of interest
- Image and face recovery

The listed technologies will be analysed and selected for the assessment, while further expanded on technologies brought in collaboration with BES-15 actions and other relevant projects.

1.3.3 PERSONA use cases and field deployments

The detailed PERSONA cases and field deployments will be clearly defined during the first months of the project (in T1.2) building on the large expertise from the PERSONA border and custom authorities (SPA, BZR, SMOI, MOPS) reflecting their real needs and interests. They will be also subject to final approval by the EAB in agreement with the consortium.

PERSONA will assess human acceptance of selected technologies used by border authorities under specific conditions or airport and land crossing border and customs checks in order to study and to extract information for the definition of the assessment method and deployments of selected technologies. As example of usage, in the context of security enforcement scenario in an airport

environment, a simulator of a control gate will be implemented to test the reaction of the users to a situation and to the solutions deployed. In this case (Figure 4 below) the “user” is tested (live environment), using different sensors (simulated e.g. TeraHertz sensor), for detection of a concealed weapon.



Figure 3 – Overview of Airport baggage handling

The results, in this case, is showed (simulation) to the person to learn and get information from the reaction. Other types of information can be shown, like the image below, to the security force person that is under test.

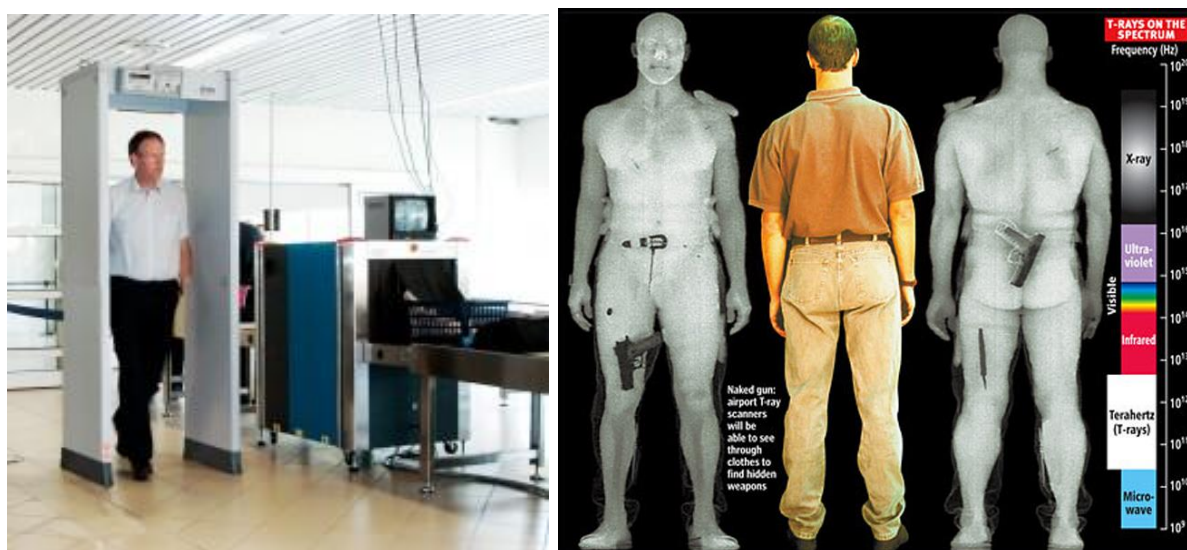


Figure 4 - Detection of hidden items

1.3.4 National/International research & innovation activities

The PERSONA Consortium recognizes the opportunity of exploiting partners experience and know-how acquired in past projects and to collaborate with other national and international projects related to security and specifically to the usage of biometrics (possibly in the area of border control) as well as ethical, privacy and data protection concerns. Hereafter, the relevant EU projects that PERSONA will enhance and with which PERSONA can establish a liaison relationship are listed.

Relevant projects	Relation/Complementarity to PERSONA

<p>ABC4EU (H2020, 2015-2018)</p>	<p>ABC4EU focuses on Automated Border Control Gates for Europe, a 17 million € European ongoing project, making border control systems more flexible. Flexibility will be achieved through automation and will cover all the different characteristics of a border control system (e-passport management, biometrics, gate design, human interface, processes and signalling). The project will also assess face and finger biometric technologies and research new anti-spoofing techniques, multi-modal fusion for these traits, as well as develop a cost-effective handheld prototype device to be used in mobile border control scenarios. Through ATOS who is key technological partner in ABC4EU, PERSONA will directly assess the solutions developed in ABC4EU. Furthermore, ABC4EU has performed impact assessment of built technologies and PERSONA will exploit the knowledge and expertise gained in this project.</p>
<p>FLYSEC (H2020, 2015-2018)</p>	<p>FLYSEC aims to develop and integrated and end-to-end airport security process for passengers. The project will integrate new and existing technologies on video surveillance, intelligent remote image processing and biometrics combined with big data analysis, open-source intelligence and mobile/RFID application. Policy, regulatory and standardisation aspects will also be examined in the context of FLYSEC innovative security concept. PERSONA will liaison with the FLYSEC project, to leverage the knowledge with respect to developed technology and engage technical partners in assessment of technology acceptance.</p>
<p>ASGARD (H2020, 2016-2020)</p>	<p>ASGARD aims to create LEA Technological Autonomy, by building a sustainable, long-lasting community form the LEA and research and development industry that will create, maintaining and evolving a best of class tool set for the extraction, fusion, exchange and analysis of Big Data including data for forensic investigation and border control. Through the INOV who is partner in ASGARD, PERSONA will leverage and exploit gained expertise and solutions developed under ASGARD project in development of the PERSONA orchestration framework.</p>
<p>ROCSAFE (H2020, 2016-2019)</p>	<p>ROCSAFE “Remotely Operated CBRNe Scene Assessment Forensic Examination”, with the goal of fundamentally change how CBRNe events are assessed, in order to and ensure the safety of crime scene investigators by reducing the need for them to enter high-risk scenes when they have to determine the nature of threats and gather forensics. Through the ROCSAFE partner INVO, PERSONA will bring and assess wide range of sensors and data analytics solutions developed under the ROCSAFE project.</p>
<p>MobilePass (FP7, 2013- 2016)</p>	<p>MobilePass focused on research and development towards technologically advanced mobile equipment at land border crossing points. This will allow border control authorities to check European, visa-holding and frequent third country travellers in a comfortable, fast and secure way. PERSONA will contact MobilePass technological partners and create synergies for assessment of developed technologies under this project.</p>

1.3.5 Gender Analysis

PERSONA does not raise any particular gender issues. For instance, all partners’ institutions apply equal opportunity employment policies. Some of the participating groups contain also a large

percentage of female group members. Furthermore, each of the partners is committed to supporting the female members of the community within this program by encouraging their participation in networks of women scientists, providing exposure to the team and technical community and mentoring them in their professional growth. This aligns with the understanding stated in the 1999 EU Research Commission's report on women in science that it is only by ensuring greater gender equality, that science will optimize the value that it brings to European society.

The PERSONA gender action planning will be based on the following directions: (a) Active participation of female researchers in the project, (b) Strengthening collaboration links to the prominent female scientists; (c) Promoting women speakers to represent the project in conferences in Europe and overseas; (d) Registering female participants in the European Database of Women Experts in SET-Science, Engineering and Technology; (e) Publishing achievements of women in the field on the project's web site(s), but also through posts in the electronic media linked to the project; (f) include equal number of male and female pilots' end-users, to capture end user profiles from both genders.

1.4 Ambition

1.4.1 Privacy and data protection aspects of border crossing

The new data protection framework intends to lower the level of the regulatory fragmentation regarding the protection of personal data. The EU data protection reform, comprised essentially of the GDPR (Regulation 2016/679) and the Police and Criminal Justice Data Protection Directive (Directive 2016/680; Directive), was only concluded on April 2016. The GDPR will become applicable across the EU on 25 May 2018; the Directive needs to be transposed into Member State legislation by 6 May 2018. The Regulation will follow the ideology of Directive, and aims to reinforce data protection rights, rather than to become an entirely new way of protection.⁶ Therefore, to assess the effectiveness and *raison d'être* of the notion of risk in the Regulation, its appearance in the Directive must be assessed beforehand. The Directive aims to protect fundamental rights, especially the right to privacy⁷, by laying down requirements regarding the processing of personal data. It does not mention the right to the protection of personal data at all since it was drafted in a pre-Charter era. The Directive (along with e.g. the Regulation 45/2001) refers to art. 8 (1) ECHR, which establishes the right to private life. As the Lisbon Treaty came into force in 2009 and art. 6 (1) TEU incorporated the Charter, furthermore the right to the protection of personal data was reiterated in art. 16 TFEU, the newly established right became binding primary law of the EU (through art. 8 Charter).⁸ Art 52. (3) Charter states that as it "*contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention.*" Although the right to the protection of personal data is not apparent as a separate right in the Convention, it can be related to some parts of art. 8 ECHR.⁹ The CJEU also interpreted EU data protection law in light of art. 8 ECHR before the proclamation of the Charter.¹⁰ The right to private life can be considered

⁶ <http://statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf>

⁷ <http://ssrn.com/abstract=2754043>

⁸ <http://idpl.oxfordjournals.org/content/3/4/222.full.pdf+html>

⁹ <http://www.sciencedirect.com/science/article/pii/S0267364913001325>

¹⁰ Gloria González Fuster, 'Curtailling a right in flux: restrictions of the right to personal data' in Artemi Rallo Lombarte and Rosario García Mahamut (eds.), *Towards a new European Data Protection Regime* (Tirant lo Blanch, Valencia 2015) 513,522



as an umbrella right which protects inter alia the individuals against the processing of information relating to them.¹¹

The aforementioned fundamental rights are not absolute rights, their limitation is possible¹², however the limitation “*must be provided for by law, respect the essence of those rights and freedoms and, subject to the principle of proportionality... are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.*”¹³ Therefore the processing of personal data constitutes a limitation of a right or freedom, as it affects the individual. However, in certain cases it is possible that the benefits outweigh the risks, thus the limitation will be allowed by data protection law.

PERSONA Privacy and Data Protection Impact Assessment (PIA and DPIA)

The appearance of DPIA in the GDPR is the outcome of several concepts, but most importantly follows the approach which targeted the implementation of an already existing form of risk assessment in the field of privacy protection, namely Privacy Impact Assessment. A privacy Impact assessment (PIA) is a process for assessing the impacts on privacy a project, policy, or Other initiative (hereinafter: project) and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise the negative impacts.

Besides Europe, the origins and different forms of PIA can be found in Australia, Canada, Hong Kong, New-Zealand and the United States.¹⁴ PIA has strong similarities with other processes which combine political, social and legal norms, as the ideology of the process shows far connection with Environmental Impact Assessments from the 1960s¹⁵ and Social Impact Assessments from the 1980s¹⁶. Major differences can be identified among the PIAs in the aforementioned countries: some have political nature, others are part of a risk management strategy of an organisation.¹⁷ PIAs – and subsequently DPIAs – emerged in the 1990s and became institutionalised, in different forms and at various levels of compulsion, first in common law jurisdictions, such as New Zealand, Australia and Canada. In Europe, the earliest policy for PIA was developed in the United Kingdom in 2007.

The proliferation of privacy- (PIAs) and data protection- impact assessments (DPIAs) is attributed to three main factors: (1) the growing invasiveness of emerging technologies into individual lives and social fabrics, (2) the increasing importance of the processing of personal data for contemporary economy, national security, scientific research and technological development, and inter-personal relations, among others, and (3) the diminishing trust in emerging technologies and the use thereof by public and private organisations. However, some 50 years after impact assessments emerged, they still do not constitute a clear-cut practice. Only in certain areas have they gained considerable experience and matured (e.g. EIA). In other areas, their identities are still being developed (e.g.

¹¹ See *Leander v. Sweden* 9248/81 (1987) para 48.

¹² Joined cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen* [2010] I-11063 para 48. Also emphasized by Recital (5) GDPR.

¹³ Art. 52 (1) Charter.

¹⁴ In Europe PIAs are conducted in the United Kingdom and in Ireland.

¹⁵ Originated from green movements in the 1960s. Read more at: International Association for Impact Assessment: Principles of Environmental Impact Assessment Best Practice <<https://www.eianz.org/document/item/2744>> [13/04/2016]

¹⁶ SIAs aim at ensuring that developments or planned interventions maximise the benefits and minimise the costs of those developments, including, especially, costs borne by the community. For more information read: The Interorganizational Committee on Guidelines and Principles for Social Impact Assessment: Guidelines and Principles for Social Impact Assessment <http://www.nmfs.noaa.gov/sfa/social_impact_guide.htm> [05/05/2016]

¹⁷ Hempel and Lammerant *op.cit.* 125



‘societal’ impact assessments or DPIAs) and other areas, calls for their introduction are constantly being made (e.g. human rights).

Furthermore, it must be underlined that the provisions of the GDPR and the relation with an optimal impact assessment are not without gaps and misconceptions. Whereas DPIA should be conducted only when personal data is processed and in case this operation constitutes a high risk to the rights and freedoms of the individual, an optimal impact assessment should not be limited to certain occurrences. Although DPIA will have a pivotal role during the application of the Regulation, it does not give proper answer the question “how to conduct a DPIA?”

1.4.2 Ethical aspects of border crossing

The PERSONA project acknowledges the importance of ethics in border control. In the EU there are numerous documents focusing on ethical standards for border guards (directly or indirectly):

- National Codes of Conduct surveyed in Part 1.
- Schengen Borders Code
- Schengen Handbook
- Updated Schengen Catalogue
- EU Charter of Fundamental Rights
- Universal Declaration on Human Rights
- EU Council Decision supplementing the Schengen Borders Code as regards the surveillance of the sea external borders in the context of the operational cooperation coordinated by the European Agency for the Management of Operational Cooperation at the External Borders. (2010/252/EU). April 2010.
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second-generation Schengen Information System (SIS II)
- DIRECTIVE 2008/115/EC of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals
- Council of Europe Committee of Ministers. 20 Recommendations on Forced Returns, 4 May 2005.¹⁸

As a number of ethical issues might arise from border crossing, these documents (along with others) will form a benchmark for the ethical framework in PERSONA. Although most documents are not specifically designated for border guard authorities, the principles and provisions of the abovementioned legal acts, code of conducts and catalogues are indicative.

PERSONA Ethical Impact Assessment

According to David Wright, *ethical Impact Assessment (eIA) is a process for identifying, examining and assessing the ethical issues arising from the development of a project, technology, service, policy or other initiative, and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimize the negative impacts.* eIA attempts to import a greater understanding of the role that specific contexts play in limiting our current understanding of technologies by focusing inter alia on autonomy, dignity, trust, fairness, security, responsibility, etc. With such an understanding, assessors should better be able to think beyond the immediately obvious

¹⁸ http://frontex.europa.eu/assets/Publications/Research/Ethics_of_Border_Security_Report.pdf



applications of technologies in development and subject to an eIA and imagine “how it is used or might be used in the future, not only by itself but as a component in a larger technological framework” (Wright 2011: 204). The eIA framework is built around four principles stipulated by Beauchamp and Childress, which serve to group values and issues for reflection: respect for autonomy (i.e. through dignity or informed consent), non-maleficence (avoiding harm through safety, social solidarity or isolation), beneficence (through accessibility, sustainability or value-sensitive design) and justice (equality and fairness).¹⁹

PERSONA will provide a thorough overview of the relevant ethical impacts of border control, categorize them and identify the suitable methods for addressing them. This step will be followed by the assessment of the impacts, by inter alia evaluating their importance, measure the potential value conflicts and conceptualise the ethical values and principles. The findings will be translated into practical recommendations which will be tested and validated through the PERSONA system. As other elements of the PERSONA Impact Assessment, the ethical framework will be also subject of continuous monitoring and review.

1.4.3 Regulatory aspects of border crossing

Privacy and data protection frameworks regarding border-crossing in Europe are fragmented as specialised EU authorities are fighting trans-border crime. Different systems and institutions are operating based on multilateral agreements, strengthened by numerous directives and regulations. While identifying the relevant societal concerns affected by border-crossing, the following systems will be taken into consideration at minimum.

1.4.3.1 EURODAC

The EURODAC system has been established through two regulations: Council Regulation 2725/2000 of concerning the establishment of “Eurodac” for the comparison of fingerprints for the effective application of the Dublin Convention and Council Regulation 407/2002 laying down certain rules to implement Regulation (EC) No 2725/2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention. The centralised system of EURODAC contains the fingerprint data of third-country nationals applying for asylum in one of the EU Member States. Its purpose is to assist in determining which Member State should be responsible for examining a particular asylum application under Council Regulation (EC) No. 343/2003 (Dublin II Regulation). Personal data in EURODAC (stored in pseudonymized form for 10 years) may be used only for the purpose of facilitating the application of the Dublin II Regulation; any other use is subject to penalties.²⁰

1.4.3.2 Schengen Information System

As a consequence of the accession of additional states to the Schengen Agreement (Benelux Economic Union, Germany and France abolished the checks at their common borders in 1985), the Schengen system was integrated into the EU legal framework by the Treaty of Amsterdam in 1999. The most recent version of the Schengen Information System (SIS II) came into operation in 2013, serving all EU Member States plus Iceland, Liechtenstein, Norway and Switzerland.

The system consists of a central system (C-SIS), a national system (N-SIS) in each Member State, and a communication infrastructure between them. C-SIS contains certain data entered by the Member States on persons and objects, used by national border control, police, customs, visa and judicial authorities throughout the Schengen Area. Each of the Member States operates a national copy of

¹⁹ <http://satoriproject.eu/media/1.a-Ethical-impact-assessmt-CIA.pdf>

²⁰ http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf



the C-SIS, known as National Schengen Information Systems (N-SIS), which are constantly updated, thereby updating the C-SIS. The N-SIS is consulted and will issue an alert where:

- the person does not have the right to enter or stay in the Schengen territory; or
- the person or object is sought by judicial or law enforcement authorities; or
- the person has been reported as missing; or
- goods, such as banknotes, cars, vans, rearms and identity documents, have been reported as stolen or lost property.

SIS-II has additional functionalities, such as the possibility of entering biometric data, photographs or new categories of alerts (e.g. stolen boats, aircrafts, containers), enhanced alerts on persons and objects, etc.

1.4.3.3 VISA Information System

The Visa Information System (VIS, established by 2004/512/EC: 2004/512/EC: Council Decision of 8 June 2004 establishing the Visa Information System (VIS)), fosters the establishment of a common EU visa policy. The VIS allows Schengen states to exchange visa data through a system which connects the consulates of the Schengen states situated in non-EU countries with the external border-crossing points of all Schengen states. The system processes data regarding applications for short-stay visas to visit or to transit through the Schengen area. The VIS enables border authorities to verify, with the help of biometric data, whether or not the person presenting a visa is its rightful holder and to identify persons with no or fraudulent documents.

According to Regulation (EC) No. 767/2008 of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (*VIS Regulation*), only data on the applicant, his or her visas, photographs, fingerprints, links to previous applications, and application files of persons accompanying him or her, may be recorded in the VIS by visa authorities of Member States (in exceptional cases police authorities may also request access).

1.4.3.4 EUROSUR

The European Border Surveillance System (EurosUR) is designed to enhance the control of the Schengen external borders by detecting, preventing and combating illegal immigration and cross-border crime. It serves to enhance information exchange and operational cooperation between national coordination centres and Frontex, the EU agency in charge of developing and applying the new concept of integrated border management. Its general objectives are the reduction of the number of illegal migrants entering the EU undetected; the reduction of the number of deaths of illegal migrants by saving more lives at sea; the increase of the internal security of the EU as a whole by contributing to the prevention of cross-border crime.

PERSONA regulatory impact assessment

PERSONA will conduct thorough assessment of the regulatory factors in existing and new-generation border crossing systems. In particular, PERSONA will assess the latest innovation in National Facilitation Program (NFP) systems substituting the previous *Registered Traveller Programme* (RTP), which allows third-country nationals who have been pre-vetted and granted access to the NFP to benefit from facilitation of border checks at the external border of the Schengen area. NFP shares the core functionality of RTP with the same aims to facilitate frequent travellers crossing the borders of Schengen member states, where biometric verification at border crossings will be dependent on other systems i.e. VIS, EES, eRP compliant documents & eMRTD documents as applicable. In order to deploy real piloting scenarios and assess a fully specified system design, two following processes will be tested:



- **NFP Enrolment process** covering the 1st time enrolment of a TCN into the registered traveler NFP system
- **NFP Facilitation at Border Control Point** - process covering the facilitation that NFP enrolment is able to provide at the border control point passing through eGate systems.

1.4.4 Social aspects of border crossing

Social impact is related to an event, experienced or felt in either a perceptual (cognitive) or a corporeal (bodily, physical) sense, at any level (individual, group, social, etc.), directly or indirectly. These different levels are affected in different ways by an impact or impact-causing action. As ‘social impact’ is conceived as being anything linked to an event that affects or concerns any impacted stakeholder group and the impact itself is deemed to be important by the affected individual or group. Additionally, it must be emphasized that social impacts are rarely singular cause-effect relationships (such as e.g. risks). There are complex patterns of intersecting impact pathways - e.g. health, wellbeing and social outcomes are always multi-factorial. Social impacts can happen the moment there is a rumour that something might happen as they can lead to speculation and speculative behaviour, evoking e.g. fear or anxiety.

Therefore, Social Impact Assessment (SIA) addresses everything that is potentially relevant to people in connection with the proposed event. SIA must identify the societal and understand how the technology will affect what is important to the stakeholders. The relevance of SIA lies in the subject of the process. Beside operating, decision-makers also need to seek and maintain a social licence in a respective area. To gain social licence decision-makers need to make a positive contribution to the stakeholders. As a return, they can be seen as trusted, socially responsible entities. To gain and maintain a genuine social licence decision-makers need to think about the contribution of their proposed actions to social development, inter alia by involving stakeholders to work jointly with them, thus facilitating positive changes. Regarding stakeholders, social development is more about facilitating change in institutions and society to reduce social exclusion and fragmentation, to promote social inclusion and democratisation, and to build capacity in institutions and governance instead of pursuing individual benefits (whereas e.g. privacy or data protection impact assessments prioritize individuals’ rights and freedoms). In order to facilitate a partners’ social benefits, SIA should be conducted in order to identify inter alia the means of cooperation.²¹

PERSONA Social Impact Assessment

PERSONA social impact assessment (SIA) will focus on assessing the social issues of border security solutions. It will adjust to the varying social concerns and issues at different points in the cycle of the proposed activity. PERSONA SIA is primarily concerned about the negative impacts, but the focus changed to the proposed activities and how they might be able to improve the benefits to communities and to decision-makers. PERSONA SIA will be considered as being the process of managing the social issues of proposed activities. SIA covers a very wide-ranging set of steps throughout the entire duration of the proposed activity and can be divided into four phases:

- Understanding the issue
- Prediction, analysis and assessment of the impacts
- Development of implementation strategies
- Design and implementation of management programs

²¹ Frank Vanclay: Social Impact Assessment: Guidance for assessing and managing the social impacts of projects

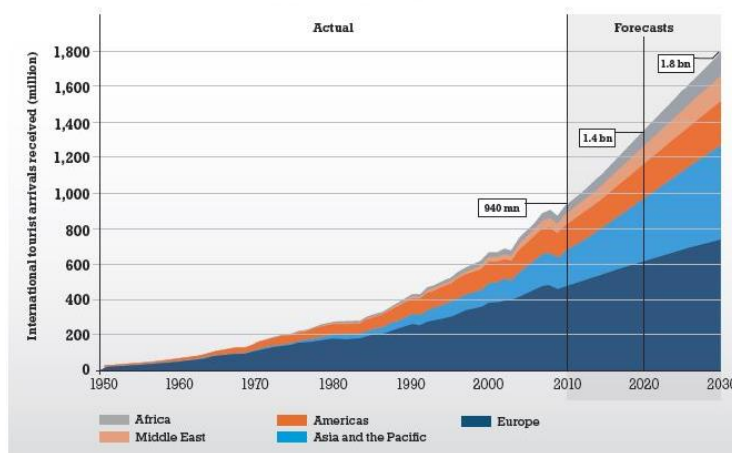


In actual practice, the tasks of managing the social issues are undertaken by a wide range of people. Therefore, responsibility for thinking about and managing social issues needs to be a core part of PERSONA management.

2 Impact

The evolution of border control security and management is one of the major challenges for countries in EU and worldwide and can have significant economic impact. In this view, the first and more direct economic impact, for PERSONA, will come from the facilitation of bona-fide travellers EU and non-EU travellers during their cross-border checks through the usage of innovative biometrics modalities for identification management and with the increase in the overall security level. Every year, more than 700 million external border crossings take place at the EU borders out of which about a third are made by third country nationals ²². The tendency for these figures is increasing due to the increased interconnectedness of the world and the needs for further interactions between countries and people. Figure 5 indicates the estimated evolution of tourist arrivals, while Figure 6 provides quantitative data concerning border crossings, including their number and type (air, land and sea), and the categories of travellers (i.e. EU/EEA/CH abbreviated as EU-citizens, third country nationals either visa-exempt (TCNVE) or visa holders (TCNVH)).

UNWTO TOURISM TOWARDS 2030: ACTUAL TREND AND FORECAST 1950-2030



Source: World Tourism Organization (2013)

Figure 5: International tourist arrivals by 2030

Efficient cross-border checking has been recognized as a factor to attract not only visitors but also multiple types of economic, business, research and educational activities, which typically necessitate regular movements to and from the EU and third-party countries. Initiatives are taken in the EU and worldwide to make cross-border checking more effective. Smart Borders, the EU initiative to manage EU external borders in a more efficient way using innovative (biometric – enabled) technologies, is expected to improve the management of the external borders of the Schengen Member States, facilitate border crossings for pre-vetted third country national (TCN) frequent travellers and provide information on over-stayers and fight against irregular immigration. The US is increasing the number of biometric passport control kiosks especially at busy airports as part of several measures to make the arrival at the country’s airports a safer and more pleasant experience.

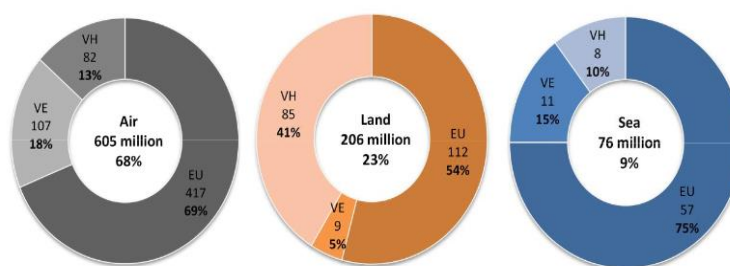


Figure 6: International tourist arrivals by 2030 (EU DG-Home Affairs, Technical Study on Smart Borders)

²² I. Enciu, Member of the European Parliament Committee on Civil Liberties, Justice and Home Affairs, Government Gazette, “European Union Border Security”

Such a continuous need calls for flexible, streamlined, automated and scalable border control systems. **PERSONA is well-positioned in this context as its main aim is to enhance the security of European borders, while further improving their crossing experience. Furthermore, biometric identification management technology, as pursued by PERSONA, is being recognized, upon a global PERSONA, as a solution for more effective and secure border control.** As demonstrated by PERSONA scenarios, the project will develop the technological modules and elaborate the procedures to support innovative cross-border checking schemas.

A second economic impact of PERSONA is the contribution to the biometrics market through the **technological progress, to be achieved in the context of the progress, in the related technologies.** The biometrics market is one of the key growing electronic security markets in the global landscape. Increasing government spending, national ID projects, e-passports & visas are spurring the market globally. The next generation biometrics market is expected to reach \$24.4 Billion by 2020, at a CAGR of 17.9% between 2015 and 2020. Travel and immigration is the leading application for the market.²³

Other estimations are converging on the expected boost: According to research, Global Biometrics Market is projected to reach \$21.9 billion by 2020. PERSONA is pursuing the advancement and demonstration of the key factors of the biometric authentication systems that feed the escalation in demand, including the improving accuracy rate, the reliability, scalability and longevity of such systems. **PERSONA covers a distinguished market need, namely to investigate, in an operational environment, more modalities (going beyond the well-established ones, such as the fingerprints) operating at the same time (in a multi-modal fusion fashion).**

As the biometrics market matures, it is expected to shift from being dependent upon stand-alone (and typically closed) products to being more evenly split across several end-use equipment segments integrated in specific scenarios. **Indeed, PERSONA is paving the way from stand-alone (and typically closed) biometrics products to new applications and integrated systems.** Successful development of the PERSONA results can drive the concept of biometrics usage in additional markets and applications, including home and office security, assisted living and e-health. Such

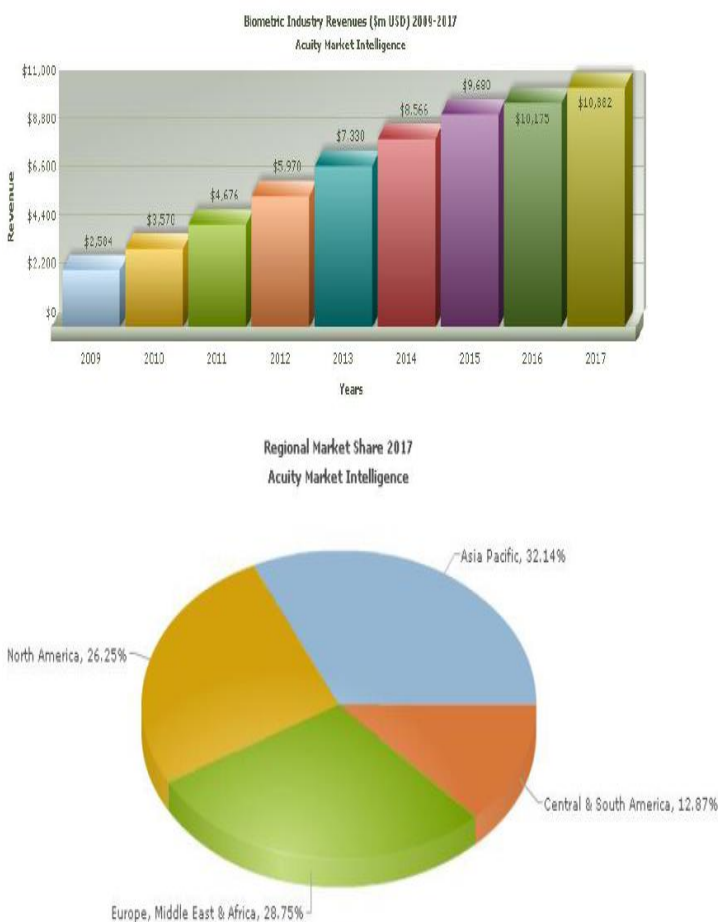


Figure 7: Biometrics market revenue estimations (Acuity Market Intelligence)

²³ Markets and Markets, "Biometric System Market by Application, Technology, Function & Geography - Global Forecast to 2020"



areas represent significant markets that PERSONA will target bringing economic impact in the context of the consortium and at the EU industry level.

2.1 Expected Impacts

The ambition of PERSONA aligns directly to each one of the listed expected impacts of the research and innovation action of SEC-18-BES-2017: “Acceptance of no gate crossing point solutions”. The success of PERSONA will be measured through the achievement of Key Performance Indicators (KPI) which will be periodically assessed throughout the project duration.

Expected Impact 1

Information systems that better manage personal information and support the automated checking and analysing of various entry and exit data, without increasing the risk of loss of privacy thanks to close cooperation with actions resulting from SEC-15-BES–2017: Risk-based screening at border crossing.

European data protection law intends to follow the trends: the recently reformed personal data protection law in the EU will introduce a requirement for data controllers to conduct an assessment of the impacts of data processing operations that are “*likely to result in a high risk to the rights and freedoms of natural persons*” with regard to the protection of personal data. This new requirement was named the ‘data protection impact assessment’ and abbreviated ‘DPIA’ and is expected to play a crucial role in the system of protection of fundamental rights in the EU. The EU has thus far put in place two sector-specific, voluntary PIA policies: the first for radio-frequency identification (RFID) applications (2009) and the second for ‘smart grids’ (2012). In the Better Regulation Package (2015), privacy and personal data constitute one of the many objects of assessment in the processes of EU law- and policy-making. After the adoption of both the GDPR and the Police and Criminal Justice Data Protection Directive (2016), a mandatory policy for impact assessment will be first introduced in the EU in May 2018 in the area of personal data protection. This development is not standalone as e.g. the Council of Europe’s recently finalised modernisation of ‘Convention 108’ and the proposed new data protection law in Switzerland (if adopted in its current wording) will both introduce a similar policy.

The PERSONA impact assessments of no-gate crossing point solutions will foster anticipatory, proactive thinking, leading to informed decision-making. Additionally, PERSONA will contribute to the protection of societal concerns as well by considering the consequences of the envisaged operation on the individual before its occurrence. To preserve its *raison d’être*, PERSONA’s impact assessment will not be based solely on one major concern (i.e. a fundamental right or freedom) as it might lead to the potential ignorance of relevant information. PERSONA is well aware that existing forms of impact assessment fall short on the effective consideration of equally important perspectives (e.g. security, privacy, data protection, etc.) undermining their efficiency. Instead, PERSONA will integrate these methods to form a wider, generic and unified impact assessment²⁴. With a clarified concept and well-defined methodology, PERSONA’s assessment method will serve as an effective tool to map and assess the acceptance of border no-gate crossing point solutions on a relevant fundamental right or freedom and other societal, ethical and regulatory concerns.

PERSONA emphasises the right to the protection of personal data. It must be underlined that the right to privacy and the right to the protection of personal data are not the same. There are

²⁴ According to the definition, established by the d.pia.lab, “*impact assessment is a tool used for the analysis of possible consequences of an initiative on a relevant societal concern or concerns, if this initiative can present dangers to these concerns, with a view to support the informed decision-making whether to deploy this initiative and under what conditions, ultimately constituting a means to protect these concerns.*” Read more at d.pia.lab op.cit.

numerous discussions about the scope and nature of these rights, however one commonly used interpretation says privacy can be used as a tool of opacity, meanwhile the right to personal data serves as a tool of transparency. The proper assessment of risks and impacts would help decision-makers, inter alia, to choose the appropriate measures to facilitate compliance or to avoid undesired consequences of their actions.

Expected Impact 2	Networks of sensors that better collect information needed for border checks, without increasing the risk of loss of privacy thanks to close cooperation with actions resulting from SEC-15-BES–2017.
--------------------------	---

Biometrics, the physiological or behavioural characteristics of humans, are recently used in a variety of fields, e.g. airport, banks, military, criminal investigations, in order to authenticate or identify individuals. Biometrics provide a very strong access control security solution, satisfying: authentication, confidentiality, integrity and non-repudiation requirements. Overall, a lot of effort is devoted in the field of biometrics, while the public becomes more accepting to their usage for security reasons, as presented below:

	In Favour	Opposed	Declined to Respond
Facial recognition for anti-terrorism at public locations and events.	86%	11%	2%
Adoption of a national biometrics-based ID system for U.S. citizens.	68%	28%	4%

Table 1 Public Acceptance of Biometrics Usage for Security [Way]

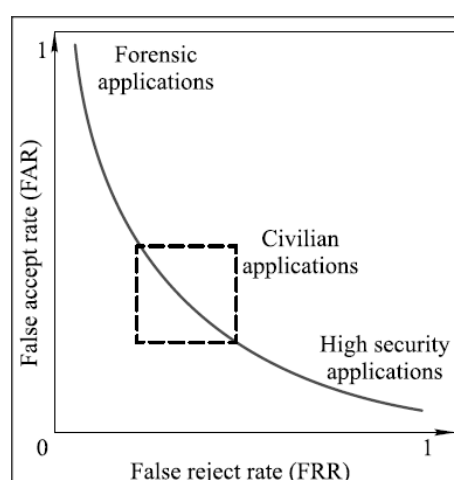
Some biometrics-based applications and their advantages/disadvantages are presented in Table 2.

Biometric	Application	Advantages	Disadvantages
Fingerprint	Access Control; ATM; Border Enforcement Agency; Check out at retail	High distinctiveness; High performance; Low cost; Short processing time; Small storage; Easy integration	Higher chance of finger image degradation by occupation, age or trauma Can be easily fooled by using fake fingerprints
Hand Geometry	Access Control; Immigration Control	Easy to use; Easy to integrate; Invariant to age; Can work with dirty hands	Accuracy is low; Fairly expensive; Doesn't work well for people with arthritis; Possibility of degradation from injury or trauma.
Hand Vein	Login control; Bank & Financial services; Military installation;	Invariant to age; Highly secure because it is hard to copy or even read	Fairly new, the effect of heart attack or other medical problems is not clear.
Iris	In law enforcement such as in prison; Airport security	High distinctiveness; High performance; Distance recognition; Low FRR; Remains almost unaffected by environmental change; Left and right iris patterns are	Not easy to use; Not easy to integrate with other system; The position of the eye can be problematic; It requires specialized devices so can be very expensive

		completely different even in identical twins	
Face	Law enforcement agencies; Banks	Can be placed on a smart card for added security; More suited for authentication; Easy to use; High acceptability	Low distinctiveness; Low performance; Sometimes background can cause problem; Can be easily fooled as by wearing a mask
Voice	Ecommerce transaction	Vocal tract is not affected by cold; Can be used with telephones; Low invasiveness; High acceptability	Local acoustics can throw off the biometric system; Age and illness can affect the voice High false acceptance rate
Gait	Security tracking applications	Can be obtained from a distance	Invasion of privacy as can be obtained from distance

Table 2: Application domains of biometrics [Nad11]

Coupled with the choice of biometric trait is also the underlying identification implementation and algorithms. These are mainly characterized by their False Acceptance Rate (FAR) and their False Rejection Rate (FRR). These two error rates are complementary. Additionally, an Equal Error Rate system is defined as a system with equal FRR and FAR. Low FRR is usually related to user comfort and as such, most civilian deployed identification systems aim for balance between FRR and FAR, thus targeting EER. Low EER's usually denote systems with high performance [Fen08, Ma09]. The IRIS system mentioned above was mostly scrapped because of its inconveniently high false rejection rate of 10%.



Each biometric trait possesses some specific properties, measuring its strength towards identification and authentication. Below is a list of the most commonly used biometric traits and their respective properties (most of them collected from).

	Face (2D)	Face (3D)	Iris	Finger	Palm	Ear	Ear (3D)	Voice	Gait
Universality	High	High	Medium	Medium	Medium	Medium	Medium	High	High
Uniqueness	High	High	High	High	Medium	High	High	Medium	Medium
Permanence	Medium	Medium	Medium	Medium	Medium	High	High	Medium	Medium
Collectability	High	Medium	Low	Medium	Medium	High	Medium	High	High
Acceptability	High	High	Low	Medium	Medium	High	High	High	High
Measurability	High	Medium	High	High	High	High	Medium	High	Medium
Circumvention	Low	High	Low	High	Medium	Low	High	High	Low

Table 3: Biometrics Properties

As depicted in Table 3, there is no singular biometric trait satisfying all the required properties at the highest level. Usually, depending on the needs and requirements of each different identification or authentication system, one of these biometric traits is chosen. PERSONA will therefore pay close attention during its study and analysis of solutions developed in BES-15 actions, to adequately address the compliance with privacy and data protection needs of European citizens.



Expected Impact 3

A method, and metrics, to assess acceptability by the society of the concept of border control processes based on "no gate crossing point solutions", and of the various technology components that may be required.

To see the full potential of PERSONA assessment method and defined metrics, the benefits and tasks to achieve these benefits should be separated. PERSONA's impact assessment will affect the decision-maker primarily, its impacts on individuals and the supervisory bodies are also noteworthy. For the decision-maker the main benefit of conducting an impact assessment is to manage future occurrences, to find the most optimal solution to a (potentially negative) future event.

Where the activity of an organization is partially or entirely regulated by legal rules, an IA can also contribute to the demonstration of compliance with certain legal provisions, thus avoid adverse consequences. Proactive demonstration of compliance can build trust and transparency, furthermore it fosters organizations to invest in compliant products and services. The following benefits are also noteworthy and should be pursued:

- **Establishing trust:** conducting an IA is not only beneficial for the decision-maker. When external stakeholders are also involved into the process, or the report of the assessment is available to open public, individuals will likely trust the organisation more. As the CNIL emphasised regarding PIAs: *"conducting a PIA will not alone bring trust from consumer and citizens. Trust will only be enabled if citizens and/or consumers are confident that these PIAs are done seriously, reviewed independently, and that additional data protection safeguards (e.g. data breach notification, etc.) are implemented."*²⁵
- **Transparency:** a possible way to gain trust is openness. The transparency of the decision-maker contributes to the empowerment of the external stakeholder (the affected person by or subject of the activity under assessment) or to regain control over technology.²⁶ The involvement of external stakeholders into the development phase can highlight the opinions and needs of the individuals, furthermore they might point out hitherto unrecognised risks.
- **Internal review:** IA serves as a preliminary compliance check and warning system. If the problematic elements of the activity are pointed out before the beginning of the operation the decision-maker can avoid complaints, fines or other adverse consequences.
- **Cost-effectiveness:** IA can also encourage the application of cost-effective solutions, although compliance with provisions and cost-effectiveness can be contradictory interests in certain cases. As the impact assessment has a proactive approach, modifications can be applied during the development, which might be significantly cheaper than during an ongoing operation. In other words: a short-term loss can end up in a long-term benefit. As costs can pose an overwhelming burden to some organizations (e.g. SMEs or startups), a noteworthy drawback of IAs should be pointed out as well. Carrying out an impact assessment is usually costly. Overwhelming financial burdens of conducting an IA could potentially prevent the decision-maker to adequately manage potentially adverse consequences or comply with legal rules.
- **Impact on liability:** According to Gellert and Kloza a properly conducted, 'good' PIA²⁷ can waive civil liability. They consider impact assessment a form of precaution through risk

²⁵ PIAF D2 *op.cit.* 36

²⁶ Lee A. Bygrave, *Data Protection Law – Approaching Its Rationale, Logic and Limits* (Kluwer Law International, London 2002) 166

²⁷ Which satisfies all its formal requirements.



assessment and risk mitigation. In case of damage, caused by a privacy-intrusive technology the person or entity cannot be held liable if he fulfilled his duty of investigation through an impact assessment.²⁸

To achieve these benefits the decision-maker should be opened to modifications and new ideas, furthermore time and workforce should be invested in the impact assessment.

For individuals/affected persons the main benefits are in close connection with the aforementioned points. A transparent organization can be considered as a trustworthy entity, who shares information about the activity and involves external individuals to the development processes. On the other hand, transparency and stakeholder engagement becomes effective only if the individuals are willing to participate actively in these processes. From a legal perspective IA can be deemed as an important tool to ensure compliance due to its preventive nature. Remedies and sanctions are retroactive and their contribution to compliance is their deterrent effect.²⁹

2.1.1 Societal impact

At a time of increased numbers of refugees seeking a safe haven in the EU and irregular migrants trying to reach Europe, with the following political uncertainty on how to tackle this, it is important to remember that Europe, its economies, societies and future prosperity, also depends on the mobility across its borders. Border control at the external borders of the EU is however a sensitive domain in several respects. Procedures of border control have to respect refugees', migrants' and travellers' rights, but also ensure their security, notably through the protection of their privacy and personal data. Another important aspect to consider when developing procedures for facilitated border crossings for frequent travellers from third countries is that the enrolment procedures in such a programme must be closely assessed in order for it to not carry requirements that directly or indirectly discriminates certain populations, violate refugees' rights to international protection or increases existing unequal access to free movement. While Europe is struggling to find out how to tackle the increased numbers of refugees and irregular migrants, its responses in terms of future border checks and general immigration policies must find a right balance between the respect for travellers' rights (notably refugees' rights) and border security.

In this quest, heightened security measures should not create an impermeable border that discourages all travellers from seeking to go to Europe, whether for business opportunities, studies, research, work, international protection etc. Indeed, in the EU context, the quality of the control of the external borders is a prerequisite for the upholding and good functioning of the Schengen area and the associated free movement of people and goods internally. At the same time, a thriving European economy also depends on the security and mobility across EU external borders. While facilitated access for certain categories of third-country nationals will not necessarily ease the current pressure of refugees and migrants seeking to reach Europe, it is likely to change the perception of European borders as being generally difficult and cumbersome to cross for any non-EU-citizen. A speedier and more efficient border control is thus likely to have several societal benefits, and in particular it has the potential to:

- Improve the travel experiences of third country nationals frequently traveling to Europe.
- Improve both the safeguarding of the rights of travellers and their security.
- Enhance the reputation of Europe as an attractive destination for business, academic exchanges and other work-related travels.

²⁸ Raphaël Gellert and Dariusz Kloza, 'Can privacy impact assessment mitigate civil liability? A precautionary approach, in Transformation juristischer Sprachen. Österreichische Computer Gesellschaft, 2012

²⁹ C-14/83 *Sabine von Colson and Elisabeth Kamann v Land Nordrhein-Westfalen*



- Enhance cross-border social and economic exchanges in regions of high levels of cross-border activities.

2.1.2 Barriers and necessary conditions

There are key barriers and obstacles set in the non-technological domains which include:

- **Political scepticism** in adopting new technologies regarding the usage of biometrics for border control. The evolution of European Policies that regulate the use of such technologies is rather slow due to the fear of compromised security or unnecessary complexing of the control procedures. PERSONA will actively pursue **public awareness** on its ongoing privacy and ethical monitoring mechanism and its privacy by design architecture through concertation, standardisation and dissemination activities, informing the public and calling politicians to action. Three workshops with training sections will be organised by the Consortium in order to create awareness and make stakeholders able to familiarise with PERSONA technology.
- **Legislative differences** at national level in terms of *the legal framework for (a) the usage of biometrics and (b) the management of privacy and ethics* for border control in the EU and abroad. PERSONA tackles this barrier by investigating any legal prerequisites in the participating countries of the EU and aligning the system requirements for ensuring **data integrity, authenticity and confidentiality**, where organizing pilots and field trials. In this context an extendable framework will be formulated that may include the needs of the other EU countries.
- **Cultural differences** in the acceptance of biometrics for border control among different EU countries. PERSONA solution employs the fusion of biometrics evidence and the support of alternative routes (matching functionality) in order to reach the confidence level. In this view these routes can be adjusted or customized to the different cultural and ethical requirements. PERSONA has dedicated a complete work package to the project's impact to privacy to validate its **compliance with legislation and ethics**.
- **Economic barriers** in the adoption of new technologies due to the reluctance of decision makers to move away from traditional systems, on which heavy investments have been placed, and invest in new ones: PERSONA will perform **cost-efficiency studies and market analyses** that will show the advantages of the proposed platform, and will disseminate the results to all stakeholders and urge them to action.

2.2 Measures to Maximise Impact

The PERSONA consortium recognizes the importance of dissemination and exploitation of the project results and the necessity of sustainability beyond the project lifetime. The PERSONA workplan dedicates resources for creating a targeted dissemination and exploitation plan (WP6). This activity strongly relies on the practical experience of cooperative projects of a number of the partners and every consortium member of PERSONA is highly committed to disseminate the outcomes of PERSONA.

2.2.1 Dissemination plan

Dissemination and transfer of knowledge will be both internal and external activities. Dissemination activities will be critical to give PERSONA the necessary visibility to end users and the scientific community. In WP6 a detailed dissemination strategy will be designed and implemented. The full initial dissemination plan will be included into D6.1 (M5). The proactive dissemination strategy will be designed to:



- **Build an active community of interest** around the project results, including target groups as:
i) Related European border and custom authorities, **ii)** Security industry, **iii)** Scientific community, **iv)** End users (airports, border crossing points etc.)
- **Disseminate information** about the technical progress and results to the security industry, border control authorities and research communities, through conferences, fairs and scholarly publications.

Dissemination actions will specifically include:

- **Documentation:** Both internal and public documents are foreseen. The former is circulated inside the project as soon as the involved partners, and work package leaders or technical manager have declared their consent.
- **Website:** An official project website as the main information hub for external dissemination will be created, documenting the goals and status of the project. The site will contain regularly updated information regarding project achievements.
- **Publications:** Academic and research partners will actively participate in international scientific conferences and workshops and publish results in peer-reviewed high profile international conference proceedings and journals, with a focus of producing open access and joint PERSONA publications. Indicatively PERSONA will focus on the following:

Additionally, all partners will promote public awareness of activities and results via the production of promotion material, pamphlets and posters, to display and disseminate project concepts and achievements.

- **EC Dissemination Mechanisms:** PERSONA will pursue dissemination and maximum networking with other ongoing relating activities by making maximum use of the EC supported dissemination mechanisms, such as publication of project information on the official sites of EC.
- **Demonstrations:** All partners will actively participate and demonstrate project results at international exhibitions, trade shows and workshops e.g. related to border, custom and security control
- **PERSONA Workshops:** Three international workshops will be organized by the PERSONA project, with the aim of increasing the awareness around the project towards relevant stakeholders of the research community, border cross authorities, industrial community, and general public. All partners will actively participate and demonstrate project results at international exhibitions, trade

Datasets and a competition session for biometrics research: PERSONA will create, document and manage datasets based upon capturing both in a lab – controlled environment and in real world settings. The datasets will be disseminated and offered to academics and commercial entities for experimentation, verification and evaluation of functional modules. Furthermore, the project will organize a competition session during the last PERSONA workshop, involving top research and commercial stakeholder in the area of biometrics to demonstrate and evaluate (based on the shared datasets) their methodologies, mechanisms, algorithms and functional modules. In parallel to pursuing synergy with distinguished researchers, PERSONA will contribute, in close collaboration and guidance by the EC, to the creation of a pan-European strategy on biometrics research.

2.2.2 Communication Activities

PERSONA recognises that there exists the danger that public is becoming disassociated from EU research, so PERSONA will focus its communication activities on regaining public confidence. Thus, PERSONA will maximise the impact of the measures identified in Section 2.2, fostering science

communication in a tangible and comprehensive way, tailored to different audience specificities and background.

Communication activities will target the general public, in order to commit the wider audience to the benefits of the European achievements. Specifically, this is targeted, initially at project launch, to inform peers and actors close to the individual project partners from all areas in order to intrigue them in the project as such and raise awareness aimed at earning their support and appreciation. As the project matures, communication of the high-level concepts of the projects will take place among this broad audience, possibly followed by tangible, interactive use-case demos. It is a goal of PERSONA consortium to continue involving the "general public" as much as possible and deemed appropriate. As PERSONA is funded by the EC public money, PERSONA consortium considers its moral responsibility to also inform the public who makes such technological undertakings and collaborative research activities possible.

PERSONA will further expand its dissemination and outreach through wide range of means including posting/updating news on the project website; releasing materials such as posters and brochures, promoting/advertising dissemination activities; publishing on the partners websites, magazines, local press, online magazines, etc.; releasing summaries and press releases; social networks and users' forum based information and marketing activities; sharing pictures, videos, comments on the social channels; advertising on TV, papers, magazines, etc. on a local scale and/or emphasised in interested communities and/or focused on relevant subjects.

Table 4 - PERSONA communication activities

Approaches	KPIs	By M15	By M30
Posting/updating news on the project website in the general area	News posts	≥ 10	≥ 20
	Views	≥ 2000	≥ 4000
Publication of support material, brochures and web site	Brochure items distributed in non-specialized audience	≥ 700	≥ 1500
	Electronic newsletter release (non-specialized audience)	≥ 1	≥ 2
Project social channels (Facebook, Google+, Twitter, etc.)	News posts in social media	≥ 60	≥ 60
	Responses/likes/views of social channels	≥ 1000	≥ 1500
Competition session	Number of events		1
	Attendees		≥ 12
Workshops/ exhibitions	Number of workshops	1	3
	Attendees		≥ 100
Objectives		- Creating awareness about PERSONA	- Solicit first market interest in the project to create demand and promote research results

2.2.3 Linking to other projects & public outreach



PERSONA consortium has recognised the value of spreading knowledge both at national and European level through the collaboration with other national and international projects related to security and specifically to the usage of biometrics (in the area of border and custom control) as well as ethical, privacy and data protection concerns. This activity will consist in creating links and synergies with “sister” projects, taking part of standardisation efforts, inviting key members of other projects to provide keynote talks or to participate in highly interactive panel discussions as part of project workshops/sessions and participating in third-party events in order to disseminate the results thus far and to seek feedback.

PERSONA workshops will be organised as part of the Task 6.4 to gather important feedback from stakeholders, shape up user and system requirements, and foster the exchange of views and different perspectives in the field. In particular, three dedicated workshops will be organised (in M10, M20 and M30) likely in conjunction with project meetings or main conferences in order to maximise impact and optimise travelling and time from partners.

2.2.4 Data Management Plan

The consortium will set up a detailed Data Management Plan as required by the H2020 Pilot on Open Research Data and maintain this throughout the project. Early in the project, the Consortium will identify a strategy in order to manage project data ensuring the compliance with the Commission policies and ethics approval requirements. Supported by the External Advisory Board members, the PERSONA DPO and the PERSONA Ethics Manager, the Data Management Plan will analyse what kind of data the project will generate or collect as well as define how to collect it, organise it, store it, secure it, back-up it, preserve it, share it and, eventually, make it accessible for verification and reuse. National authorities will be notified in case of processing of personal data. A dedicated server will be used in order to host relevant research data in VUB’s Data Center, where the previously identified rules will be applied.

Moreover, an on-going monitoring of the impacts of the PERSONA project and the technologies it will develop on the Ethical, Regulatory and Social Acceptance (ERSA) requirements identified in WP2 will be performed by partner PRIO, supported by partner VUB. This will ensure the compliance with ERSA requirements and will advise against any activity/action incompatible with them.

Finally, in accordance with the requirements to disseminate the results and developments of the project, the Project Coordinator (PC) will ensure that all public documents (deliverables and publications) are made available to the public. These documents will include reports, papers and presentations marked for public dissemination and will also include confidential documents, where sensitive material can be removed. In addition, any data generated (including, but not restricted to, the following material: video material covering experiments, biometrics datasets, demonstrations and trials, simulation results, presentations, promotional material, press releases etc.) during the development of PERSONA will also be made publicly available (if applicable), subject to IPR protections, and will be collectively hosted on a permanent repository for the project’s outputs upon PERSONA conclusion.

2.2.5 Exploitation of Project Results

Two complementary visions will be implemented, i.e. a project global market objective and partners exploitation initiatives. Performed in Task 6.5, this will align with project workflow, taking into account privacy, ethical, regulatory and social assessment methods and procedures, deliverables, reports, and no-gate crossing points solutions implemented and tested in PERSONA.

The PERSONA outcome will allow for immediate exploitation of the project results and the know-how acquired. While each partner will develop its own exploitation plans, a common plan will be defined during the project course in order to build on the collaboration effort achieved and allow for a strong Pan-European move towards detailed guidelines and important assessment outcomes for EC and decision makers. Unsurprisingly, LEAs constitute the natural market for the PERSONA ecosystem. There is no better promotion than done between peers, i.e. the LEA partners of PERSONA explaining the operational benefits to their colleagues of the different countries in dedicated conferences, in the demonstrations organized or bi- or multi-lateral cooperation. At a second level, the research partners will present and document the integrated solutions derived from the project, the way the different individual solutions of the partners should be integrated and all the support options the potential end-user will benefit from.

Individual exploitation plans of PERSONA consortium

As discussed above, PERSONA partners play a crucial role in a successful exploitation of the results and outcomes of the project. The following table summarizes the measures taken by each partner for industrial and commercial exploitation.

Partner	Planned Exploitation
VUB	VUB, as a non-profit research institution, is primarily interested in fostering the research on impact assessment methods related to border-crossing, realised by PERSONA, on inter alia privacy, data protection, societal acceptance and ethical principles (as well as on other relevant societal concerns) with an aim to devise best way and procedures guaranteeing the respect for such rights and principles, especially in the light of the reform of the EU data protection framework and of the Council of Europe’s Convention 108 on data protection. The impact assessment method developed undertaken within the FORESTOR project will enrich VUB knowledge and experience in a field, with positive impact on further research, teaching and consultancy. Also, VUB’s experience might contribute to the creation of standards with respect of the framework for privacy and data protection impact assessment.
PRIO	Considering the monitoring and review role of PRIO in the project - most of the output of PRIO will be for internal use only. Additionally, PRIO will participate in international publications and workshops when relevant to their role in the project. In addition, PRIO will also leverage the strategic positioning of its international cooperation with external organisations to initiate bilateral dialogue with policy makers.
CEL	Project outcomes and the knowledge acquired during the project will enrich CEL offering in the educational field as well as in the consultancy services for clients such as the public administration (e.g. municipalities, companies participated by public funding) or private companies (e.g. small, medium and big industries). Such services aim to help clients comply with European and national legal frameworks, in particular with regard to the new General Data Protection Regulation in May 2018, promoting transparency and trust when offering their own services to customers/citizens.

<p>ATOS</p>	<p>The following sample set of Atos solutions and capabilities will mainly benefit from the outputs of the PERSONA project:</p> <ul style="list-style-type: none"> ▪ Electronic Machine Readable Travel Documents (eMRTDs) ▪ eGate which is based on the Homeland Security Suite from Atos IT Solutions and Services ▪ Data Capture, Validation, Checkpoint Application, and eGate Application <p>For the PERSONA project Atos will search and propose innovative interaction between human and technologies, keeping in mind reaching improved modern solutions providing time efficient, secure and great boarding place to work and pass through (either as a border control staff or a passenger). It will be a great benefit for Atos to implement these crucial findings in its solutions and services.</p>
<p>INOV</p>	<p>INOV plans to exploit the project results by using the know-how gained through the action to improve its existing solutions and products (in order to get them at the required maturity level). INOV will also explore new business opportunities, either related to the project itself or to the technologies developed and demonstrated by the Consortium. INOV will also continue collaborating with the Consortium partners, providing consulting and technical support in the demonstrations and/or implementation of the developed technical solutions and pursuing emerging business opportunities. As a non-profit research and technology institute with strong links to Portuguese technical universities, one important result of the participation in the project will be to increase the expertise in risk assessment, cyber-threats and incidents, namely increasing the academic and research skills of the participants and transferring this knowledge to the Portuguese universities and industry.</p>
<p>QMUL</p>	<p>The participating QMUL/MMV specialises in forensic data analysis and will exploit PERSONA outcomes to reinforce its position in the competitive UK Research Assessment Exercise, extending its ability to generate new research funding from other sources and strengthening its consultancy services. QMUL also wholly-owns Queen Mary Innovation Limited (QMI), which is a subsidiary whose core business activity is technology transfer and the management of QMUL's SMEs and spinout portfolio. Furthermore, QMUL benefits from a long-term partnership with IP Group plc, a private equity investment company based in the City of London that works closely with QMI to identify and develop new business opportunities arisen from this project.</p>
<p>SPA</p>	<p>The outcome of the PERSONA project will be exploited by SPA in form of</p> <ul style="list-style-type: none"> • Improved passenger cooperation, self-servicing, training • Border control staff cooperation, performance, management and training, • Border control staff, passenger and technology collaboration and interaction, • Improved decision-making processes and design guidelines in smart border solutions.

BRZ	The main exploitation plan of the PERSONA results is to enhance procedures for activities of customs, especially improving the experience of people being checked and controlled on the border crossing points. BRZ will gain insights into the assessment of recent and future technology, and implement the outcomes of the PERSONA guidelines, in particular identified risks, mitigation measures and best practises on dealing with individuals crossing the border.
SMOI	The Serbian Ministry of Interior contains a large portfolio of state administration including the border crossing checks, staff training, protection of Serbian sovereignty against malicious activities through detection and prevention of illegal activities. The outcome of PERSONA will enable SMOI to adopt best practices developed within the project and strengthen the policies and procedures for border control checks. The adaptation of new regulations on no-gate crossing technologies will facilitate seamless mobility of European personnel across the state borders between the Schengen and non-Schengen states. The SMOI will also exploit the deployment of field trial reports to create specific case studies for the personnel mobility across EU.
MOPS	Experiences and knowledge gained during the scope of PERSONA will be applied in the daily tasks and mission and subsequently will also be exploited in other activities of MOPS. The results will be presented at conferences and other outreach activities with security stakeholders and border control representatives where applicable. MOPS will actively promote the promote the technological assessment outcomes to other partner nations and state officials and will leverage the knowledge to draft policies on personnel mobility at international conferences and meetings.

2.2.6 Research Data and Intellectual Property Rights (IPR) Management

The PERSONA project will be implemented based on a variety of background components and open source components. The PERSONA coordination and the Exploitation Manager (who supervises IPR issues) will perform the monitoring of the PERSONA IPR activities and IPR work. The assessment of Intellectual Property Rights involves mapping the IPRs in view of the PERSONA deliverables (as a basis for providing stronger and more practical IPR agreements for these specific IPRs when needed). In general, tools, methodology documents, benchmarks and case-studies will be available to all; some proprietary tools and algorithms may be available at the discretion and terms and of their respective owners. Based on the Business Plan analysis the consortium will decide if the commercial exploitation will be performed within the consortium members companies offering specific business contracts to contributors or a spin-off company needs to be created. Finally, all knowledge will be managed in accordance with the Horizon2020 Grant Agreement and project Consortium Agreement. Foreground Management will be based on modern methods such as BSCW (<http://www.bscw.de/>), LifeRay (<http://www.liferay.com/>), on the private area of the PERSONA webpage/portal, which will allow cooperate work on “living” documents. The PERSONA consortium will strive to deliver components developed within the project duration under open source policy with the proper license scheme to protect the background and generated IPR. Specific pieces of software or applications used for testing or validation purposes may be released as libraries or executables. IPR Management during the project: For the success of PERSONA project, it is essential that all project partners agree on explicit rules concerning IP ownership, access rights to any



Background and Foreground IP for the execution of the project and the protection of Intellectual Property Rights (IPRs) and confidential information before the project starts. Therefore, such issues will be addressed in detail within the Consortium Agreement between all project partners. Access Rights to Background and Foreground IP during the project: To ensure a smooth execution of the project, the project partners agree to grant royalty-free access to Background and Foreground IP for the execution of the project. This will allow the researchers the ability to execute the project to the best of their ability, without being hindered by administrative issues. All project partners will determine any Background IP they are willing to submit to the project within the Consortium Agreement before the project starts. Details concerning Access Rights to exploitation to Background and Foreground IP will further be defined in the Consortium Agreement.

Consortium Agreement: The management of PERSONA's background and foreground knowledge will be specified in the Consortium Agreement, following well-known models, such as DESCA 202 (<http://www.desca-2020.eu/>). The purpose of the Consortium Agreement is to establish a legal framework for the project to minimise any internal issues within the PERSONA consortium related to the work, IP-Ownership, Confidential Information, Access Rights to Background and Foreground IP for the duration of the project and any other matters of the Consortium's interest. The consortium agreement will be drafted in such a way that it is possible for all partners to carry out their project activities whenever it is dependent on transfer of knowledge from other partners, whether this is foreground or background knowledge needed for the execution of the project. The consortium agreement will protect the legitimate IP interest of all partners by explicitly limiting the rights to background knowledge and where required, even limiting the rights to foreground knowledge developed during the project when there is no need-to-know or need-to-use.

IPR management: Foreground IP shall be owned by the project partner carrying out the work leading to such Foreground IP. If any Foreground IP is created by at least two project partners and it is not possible to distinguish between the contributions of each of the project partners, such work will be jointly owned by the contributing project partners. The same shall apply if during carrying out work on the project, an invention is made having two or more contributing parties contributing to it, and it is not possible to separate the individual contributions. Any such joint inventions and all related patent applications and patents shall be jointly owned by the contributing parties. In order to further the competitiveness of the EU market, and to enhance exploitation of the Consortium Results, each contributing party shall have full own freedom of action to exploit the joint IP as it wishes, and further the goals of the consortium. To promote this effort the contributing party will have full own consideration regarding their use of such joint Results and will be able to exploit the joint IP without the need to account in any way to the other joint contributor(s). Any details concerning the exposure to jointly owned Foreground IP, joint inventions and joint patent applications will be addressed in the Consortium Agreement.

Transfer of Results: As results are owned by the project partner carrying out the work leading to such Results, each project partner shall have the right to transfer Results to their affiliated companies without prior notification to the other project partners, while always protecting and assuring the Access Rights of the other project partners. Such use of Results will encourage competitiveness of the EU market by creating broader uses of the Results and opening up the markets for the Consortium's Results in all markets.

Additional information on Consortium Agreement and IPR Management are available at Section 3.2.

2.2.7 Contribution to Standards and International Initiatives

In order to meet this growth in passenger flow and air traffic, automated border control (ABC) systems have been installed at different worldwide airport entries and exits with the aim of



facilitating travel while maintaining the security of international border crossing points. In an effort to work towards harmonization, several practice guidelines have been published by different organizations, such as Frontex (technical and operational), Inter-national Civil Aviation Organization, the International Air Transport Association, and the European Committee for Standardization. The European Union had been made also some effort in order to harmonize and enhance the workflow of the ABC e-gates, funding several European projects for example FastPass and ABC4EU, which will produce future guidelines. The objective is to create a definitive guide to ABC specifications and design based on human-computer interaction and safety aspects, maintaining a high level of quality and inter-operability between systems and subsystem. Each ABC subsystem and subsystem are subject of a group of standards proposed by the above organizations, for example, regarding facial images, ICAO requirements, for second generation systems, they should follow the ISO/IEC 19794-5, and for facial capture the false rejection rate (FRR) should be less than 5%. The PERSONA team has a good in-depth experience in the successful development of such a standard, with its partners (ATOS, INOV and QMUL) instrumental in the elaboration of ISO 22311 Societal Security – Video Surveillance – Export Interoperability and its promulgation in 2012. This standard was developed because LEA investigators were routinely faced with CCTV pieces of evidence they had major difficulties to play, localise, synchronise and etc. This standard started to be called in the procurement specification written by the operators, because it is recommended by their local authorities or just because they have good reasons to think that their options will be future-proof (a key point when your assets have a 30+ life expectancy).

ISO has recently reorganised its security-related activities into ISO TC 292 Security and Resilience with a working group (WG 6 Security) ready to host further technical interoperability developments made on the request of the LEAs. WG6 has in fact already decided earlier in 2015 to upgrade and expand ISO 22311 with a refined scheme for metadata describing the video scenes with a section on interoperability of the analysis algorithms (video input, but also in the indexes produced), with test methods, etc. There is a significant conjunction between the work to be done on the PERSONA Common Data Model and the above metadata standard; a similar synergy applies to the minimum interface requirements applicable to the developed tools. The plan is accordingly to, directly and early in the project, support with PERSONA outputs the ISO 22311 upcoming activities and propose New Work Items (NWI) to WG6 as soon as a stable consensus is reached within the Project on the need of a dedicated topics where trans-border timely cooperation is crucial, like sharing the format to describe the interoperable forensic databases in a unified way. It must be noted that security-oriented standardisation activity is always performed in close cooperation and under a formal liaison with the groups active on this same speciality for general purposes in the latter example it would be probably be done in cooperation with SC 27 Cyber Security. It is also noteworthy that going directly to ISO effectively permits a worldwide consensus and that international agreement permits an automatic translation into a European standard. In particular the following contributions will be carried out by PERSONA partners, who are already active among the standard bodies.

3 Implementation

3.1 Work Plan — Work Packages, Deliverables and Milestones

The PERSONA work plan has a duration of 30 months and has been structured into 7 work packages to appropriately support the envisioned ambition of PERSONA in developing methods and procedures for assessment of no-gate crossing point solutions with respect to the privacy, ethical, regulatory and social aspects. As a research and innovation action, the workplan follows a continuous monitoring of PERSONA activities with periodic validation of scientific innovation. The workplan is structured in such a way that the development of PERSONA outcome is constantly monitored and driven by the requirements of users and stakeholders brought together via dedicated communication means.

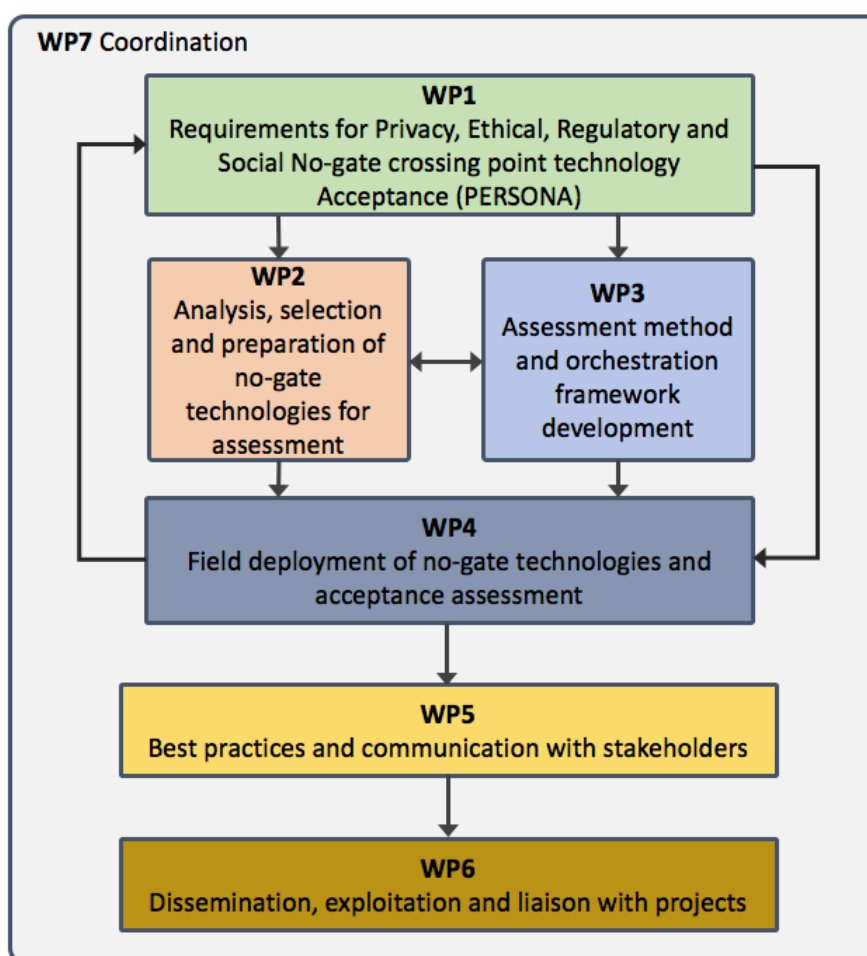


Figure 8: Organisation of PERSONA activities

In more detail, WP1 covers the user and technical requirements for PERSONA assessment, monitoring of results from these assessments against the requirements and identification of risks and mitigation actions. WP2 focuses solely on technical part of the project, studying existing solutions developed in BES-15 actions and other relevant projects, but mostly dealing with preparation of PERSONA no-gate crossing point solutions, bring technologies to the minimum of TRL5 level, tuning and optimising these technologies for the assessment and performing validation tests. One of the most important outcomes of the PERSONA project is a unified assessment method which will be carefully designed by dedicated PERSONA partners. This work will be executed in WP3, accompanied by definition and development of the orchestration framework enabling user friendly assessment of the selected technologies. WP4 is dedicated to the planning and execution of the field deployments where with help from PERSONA border and custom authorities the actual

assessments of solutions will be carried on in the most realistic environments. WP5 represents the final objective of the PERSONA project, where dedicated network and board of key decision makers, practitioners, border and custom authorities, social scientist, service providers and other important stakeholders will be established, and via various online tools and physical meetings during organised workshops, the bilateral communications will be carried out about the outcomes from the PERSONA project, in particular about best practises and guidelines.

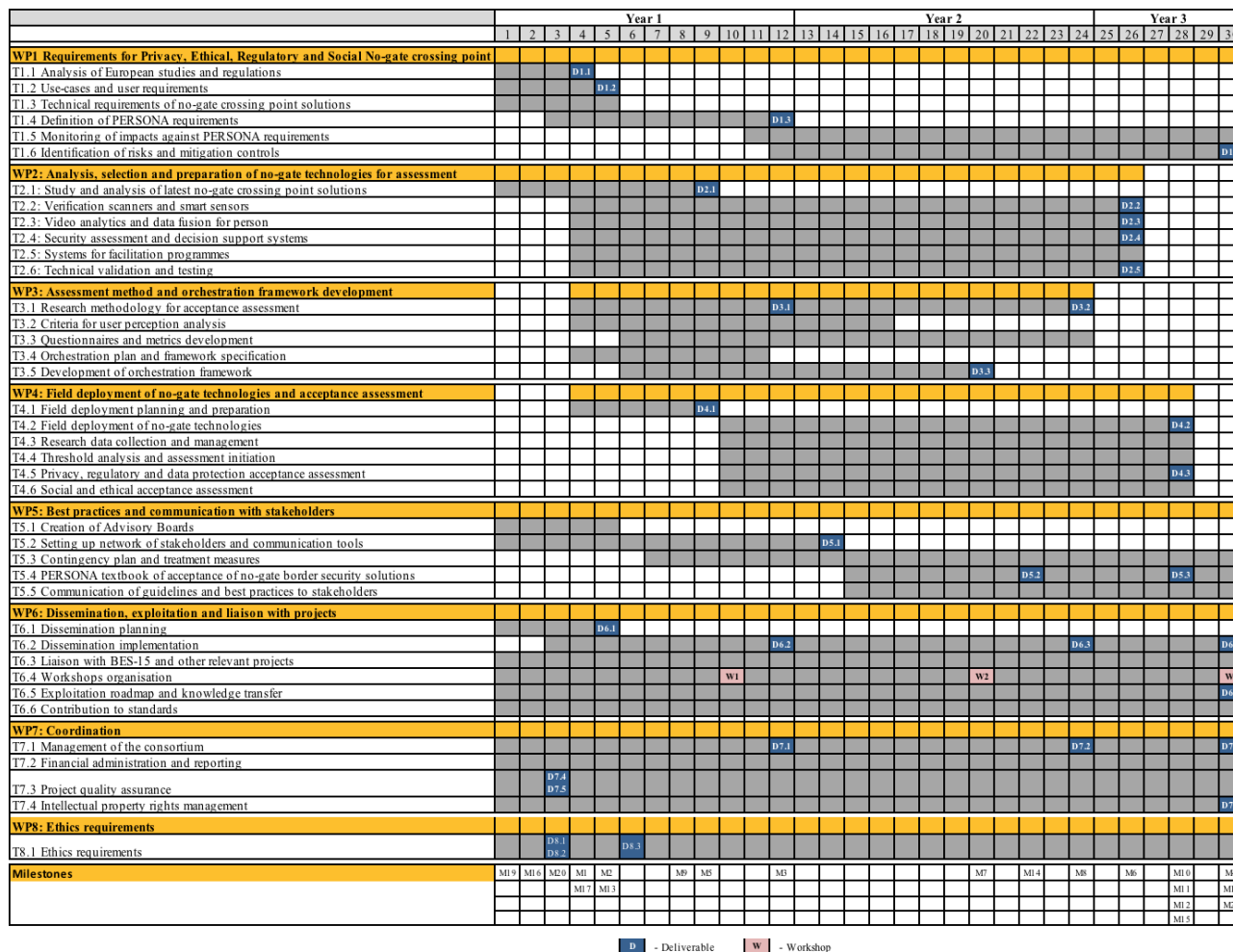


Figure 9: PERSONA Gantt chart

The ultimate outcome of the PERSONA project will be publicly published textbook of assessment of no-gate crossing point solutions. WP6 is another important work package where all important means for dissemination and outreach will be designed and put into use. Here, PERSONA will communicate with different audiences, but mostly create close synergies with BES-15 actions, other EU relevant projects, and leading European services providers. Dedicated workshops will be organised here, and roadmap towards exploitation and standardisation will be paved. The overall project coordination is carried out in WP7 with the concrete task on IRP management. In Figure 9, an overview of the workplan along with expected outcome of each WP and task is presented. The workplan is constructed to allow for task level interdependencies that enables systematic development of PERSONA assessment method and the actual execution of the assessment on the wide range of selected technologies. A more detailed breakdown of the workplan with technical task descriptions are provided subsequent Tables.

3.2 Management Structure and Procedures

PERSONA will use a clear and efficient management structure (see Figure 10) tailored to the special needs of the project. Due to relatively small number of partners, there will be a close and strongly

linked collaboration per se. In order to be successful a functional organizational structure must be in place that ensures efficient, result-driven management. The PERSONA management structure and procedures have been carefully designed to effectively support a 30-month research and innovation project, well-organised operational teams and specialised roles to ensure synchronisation of project priorities. The plan has drawn on the coordinator’s and partner’s experience in running a broad selection of EC funded projects, including several of large-scale.

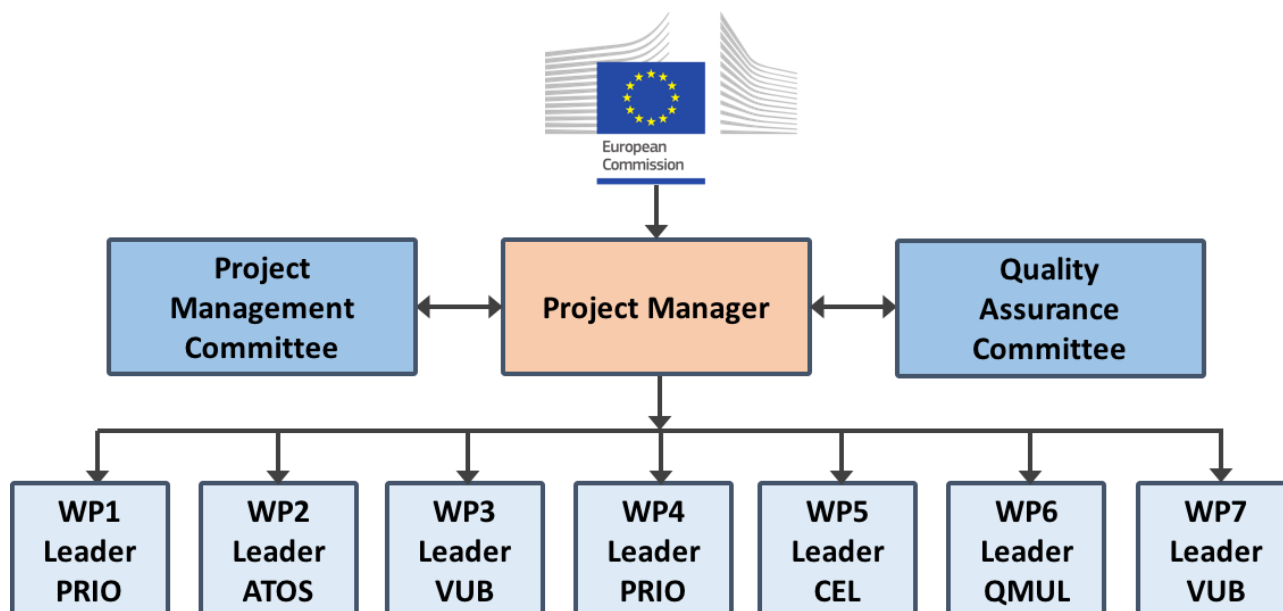


Figure 10 - PERSONA management structure

3.2.1 Governance

The organisational structure is outlined in Figure 10 with the responsibilities and interaction flows.

3.2.1.1 Project Manager (PM)

The role of the project manager will be taken by István Böröcz. As a project manager he will be responsible for the following (amongst other tasks defined by the EC Grant Agreement and the Consortium Agreement), such as a) Monitor project progress on a daily basis for continuous rating of the achievements and objectives with global view of the overall project; b) provides the Project Management Plan, which describes the project management structure, procedures for communication, cost statements, control project progress and risk management; c) quality procedures and assurance; d) coordination of communication and representation of the consortium to the EC; e) oversees the distribution of funding (according to Grant Agreement) and financial monitoring; f) document transmission to the EC, all contractual documents and reports related to the administrative, financial, scientific, and technical progress of PERSONA.

3.2.1.2 Project Management Committee (PMC)

The PMC will consist of one representative from each project partner. It has the responsibility to monitor the overall progress and direction of the project, the resources used and the costs incurred. Any deviation from the work plan should be identified by the PMC and necessary corrections have to be agreed by the PMC. The PMC is the highest decision-making body on the project. Members of the PMC should have sufficient seniority to take binding decisions, without necessity to refer back to higher authorities in their organisation. For this purpose, each project partner nominates its PMC member and a deputy at the beginning of the project. In addition to the nominated partners, the



PM and the Quality Assurance Manager (QAM) will be also members of this board. The PM will act as chairman of the PMC.

3.2.1.3 Quality Assurance Committee (QAC)

It supports the PMC in all quality related issues. It is headed by VUB and is responsible for reviewing and ensuring the quality of all deliverables, milestone achievements and project results. It is also responsible for ensuring that the roadmap to commercialization is strictly followed in compliance with the exploitation plan developed in WP6. From the outset, it will provide a handbook containing all quality assurance guidelines, processes and templates.

3.2.1.4 External Advisory Board (EAB)

The main objective of this body is to advise the consortium about the right requirements to consider and correct direction of innovation to ensure that the outcomes are valuable and will have impact and market uptake. The members of the Advisory Board listed below are selected to cover all dimensions of the project:

- Diana Alonso Blas, Data protection Officer and Head of the Data Protection Service at Eurojust, Hague, Netherlands
- Dimitrios Gkritzapis, police Major of Hellenic police Headquarters in Office of Border Protection, Division, Ministry of Public Order and Citizen Protection (Greece).
- Francois-Xavier Laurent, Head of R&D biology department, Institut National de Police Scientifique, France
- José M. Rábade Roca – Chief Officer at Madrid Municipal Police, Spain
- Chad E. Martin – Chief of Hannover Borough Police Department, Germany
- Prof. Silvia Ciotti, EuroCrime, France
- Gabriele Juodkaite-Granskiene, Forensic Science Centre of Lithuania, Lithuania
- Prof. Zeno Geradts, Nederlands Forensisch Instituut, European Network of Forensic Science Institutes – ENFSI, Netherlands

The list of AB members will be updated and expanded during the first 3 months of the project.

3.2.1.5 Security Advisory Board (SAP)

The SAB consists of experts of the end-user partners in the PERSONA consortium. The members of the SAB – by reviewing the project’s work, offering advice on specific issues concerning its subject-matter and actively taking part in certain events, namely workshops and roundtables – will contribute to the project’s development and will ensure high quality of its work. Furthermore, based on their knowledge regarding security issues, they will assess all deliverables and in particular those of WP2 prior to dissemination outside of the consortium, filtering out sensitive information.

3.2.1.6 Work Package Leaders (WPL)

The progress in the project will be evaluated by the PMC in collaboration with the responsible WPL on basis of the list of deliverables and list of milestones. The WPL is responsible for coordinating all activity and technical development in their work package and monitor the progress of the work by the task leaders and the other partners involved in the WP. In particular, the WPL takes care of timely preparation, finalizing and release of the deliverables as well as the compliance with the milestones.

Role	Name	Role	Name
WP1 Leader	Ms. Stine Bergersen	WP5 Leader	Mr. Antonio Fiorentino
WP2 Leader	Mr. Pedro Soria-Rodriguez	WP6 Leader	Prof. Ebroul Izquierdo

WP3 Leader	Mr. István Böröcz	WP7 Leader	Mr. István Böröcz
WP4 Leader	Ms. Stine Bergersen	WP8 Leader	Mr. István Böröcz

3.2.2 Research and Innovation Management

PERSONA will ensure effective research and innovation management, through a dedicated R&I Board (RIB), chaired by the Exploitation Manager and composed by the Project Coordinator and the Technical Coordinator. Additional members will be added to consider factors internal (project scope) and external (stakeholders). RIB duties will be to ensure that PERSONA research and innovation potential is continuously prioritised in the project's continuous development and realise:

- Strategic Innovation: obtain and analyse the feedback from the stakeholders, advisory groups, events and alliances as well as EC representatives to identify significant opportunities and make informed decisions about the most promising paths to achieve PERSONA goals.
- Research and Scientific Innovation: ensures that the project's results can ensure its innovative character, resolving any technical problems found during the development phase of the project.

3.2.3 Decision making and conflict management

In general, it is expected that the procedures derived from overall ongoing and coordinating tasks will be followed by each WPL and that conflicts will be solved bilaterally. In the exception circumstances when conflicts cannot be solved on WP level, the TMC may be called by the respective WP Leader and asked to resolve the conflict. In case unanimity could not be reached, decisions will be made on the basis of a qualified majority of 2/3 of the authorised representatives of the partners either present or represented by delegates. In case the qualified majority could not be reached, the conflict will be upgraded to the next higher level (the General Assembly).

Within General Assembly (GA), decisions are taken with simple majority (1/2). In case of equal votes, the vote of the PC will count for an additional decisive vote. This procedure will be described in more details in the Consortium Agreement, which along with the Contract, will constitute the basis upon which the project will be managed. To cover legal issues related to roles and responsibilities of the project participants, project management, ownership, commercial rights, exploitation, dissemination of the project results, confidentiality and intellectual property rights, a Consortium Agreement will be signed before the beginning of the project by each partner. The specific provisions will comply with general rules set out in the contract proposed by the European Commission. The Consortium Agreement will also identify relevant background of each of the partners that may be used to achieve the project objectives. The corresponding list of patents at disposal of the partners for the duration of the project will be included.

3.2.4 Reporting and communication

The organisation of the project in 8 work packages is designed in order to carry out the work and project early results in the most effective manner possible. Work packages will have regular planned teleconferences and meetings; WP teams will meet periodically to check progress and also cross-WP meeting and working groups will be planned as needed according to PERSONA needs and workplan. PERSONA will put in place communication mechanisms supporting this project structure including but not limited to: document repository, effort reporting, address book of partners, assignment of document reviewers etc. and collaboration tools such as wikis, blogs and forges. As part of communications management activities, the PERSONA strategy set out KPIs to measure

progress, monitoring and reporting and re-planning to adjust workplan. The procedures will be defined to ensure good communications, cooperation and understanding between the partners.

3.2.5 Quality monitoring

The project management strategy will be defined in D7.4, which will be the top document for project management purposes to ensure the best quality of results. The plan will set out the organisation for project management and define the key criteria for planning and control of the technical work, the budget and the programme. This Management handbook will be practical guideline to facilitate the management of the project for all participants. It will detail and explain all contractual rules and management procedures. It will provide useful advice and management tools, which will help project participants to do what is required in due form and in due time. The PERSONA progress will be monitored and reviewed against the work plan and ensuring quality and also check KPIs monitoring for success.

3.2.6 Risk Management

Risk plan and risk management in the context of PERSONA needs to ensure that potential risks are clearly identified and assessed and that the project prepares for recovery actions if required. It is known that in large, complex and relative long projects where many partners are involved, it is unavoidable that problems occur from time to time. We have performed a first PERSONA risk identification and set out measures to manage risks the contingency plan and the related WPs.

3.3 Consortium as a Whole

The PERSONA consortium is composed of 10 balanced and consistent partners representing 9 European countries: Belgium, Norway, Italy, Spain, Portugal, United Kingdom, Sweden, Austria, Serbia and Israel. All members of the consortium have a clear role within PERSONA project that complements the skillset of each other and adds value for collaborative partnership among the consortium. The

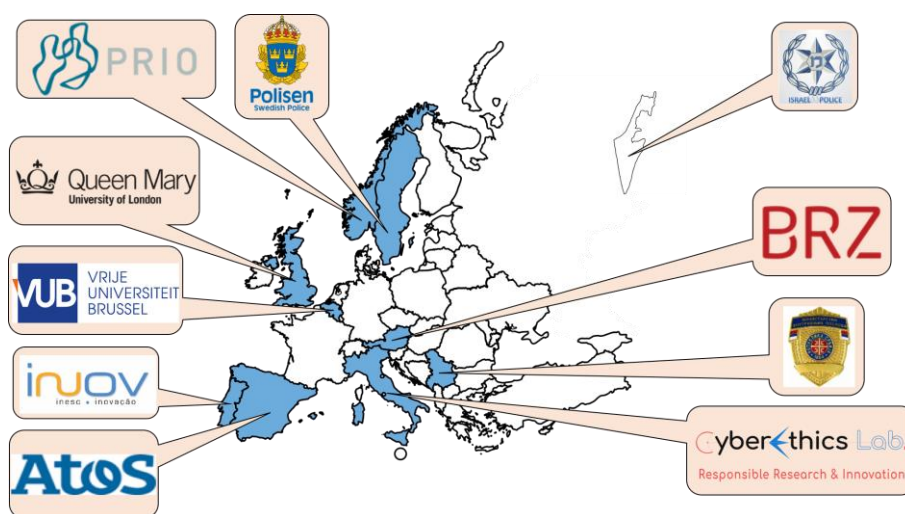


Figure 11 - PERSONA Consortium

technical background of the project consortium extends to include the full expertise and knowledge required to achieve all the goals and objectives set forth in PERSONA.

3.3.1 Complementarity of participants

The PERSONA consortium has been strategically selected to incorporate the necessary research and innovation experience, economic power and end-user representation to successfully implement the project goals. The following table presents in more depth and on a per-partner basis for all key information regarding each partners' role, expertise, expected inputs, skills and more importantly to highlight the complementarity of partners' skillset.

<p>Vrije Universiteit Brussel (VUB)</p>
<p>As coordinating partner, VUB will drive the innovation home by leading the management and coordination (WP7), ethics requirements (WP8) and assessment method and orchestration framework development (WP3). Furthermore, VUB will also lead tasks throughout PERSONA including: defining requirements (T1.4), user criteria and acceptance (T3.1), (T3.2) and questionnaires and metrics development (T3.3). With a well-established reputation in research concerning privacy and data protection, VUB will also lead privacy, regulatory and data protection acceptance assessment (T4.5), and contribute towards threshold analysis and assessment initiation (T4.4), and social and ethical acceptance assessment (T4.6). In WP5, VUB will lead the contingency plan and treatment measures (T5.3), PERSONA textbook of acceptance (T5.4), and will lead workshop organisation in WP6 (T6.4).</p>
<p>Institut for Fredsforskning Stiftelse - Peace Research Institute Oslo (PRIO)</p>
<p>PRIO is a key institution within peace research with a primary mission to conduct high-quality academic research on conditions for peaceful relations between states, groups and people. PRIO, the Security Research Group coordinated 3 FP7 projects and partnered in 8 other projects dealing with various security topics. PRIO's vast experience will thus facilitate achieving PERSONA outcomes through leading requirements for privacy, ethical, regulatory and social no-gate crossing point technology acceptance (PERSONA) (WP1), including leading analysis of EU studies and regulations (T1.1), monitoring of impacts against PERSONA requirements (T1.5), identification of risks and mitigation controls (T1.6). PRIO will also lead field deployment of no-gate technologies and acceptance assessment (WP4) as well as the threshold analysis and assessment initiation (T4.4) and social and ethical acceptance assessment (T4.6).</p>
<p>Cyberethics Lab (CEL)</p>
<p>CEL will contribute to the project supporting the promotion of the project innovation and project's outcomes uptake on the market. CEL will also participate in the project activities related to the assessment of ethical and legal concerns. CEL are well equipped to lead, best practices and communication with stakeholders (WP5) including the creation of the Advisory Boards (T5.1), creation of network of stakeholders and decision makers (T5.2), and communication of guidelines and best practices to stakeholders (T5.5). CEL will further contribute their legal and ethical awareness expertise through participating in tasks throughout WP1, plus (T4.4), privacy, regulatory and data protection acceptance assessment (T4.5), social and ethical acceptance assessment (T4.6).</p>
<p>Atos Spain S.A (Atos)</p>
<p>As a global leader in digital transformation with cutting-edge technologies, digital expertise and industry knowledge, Atos supports the digital transformation of its clients across various business sectors. Atos are thus ideally positioned to lead the analysis, selection and preparation of no-gate technologies for assessment (WP2), and specifically leading security assessment and decision support systems (T2.4) and systems for facilitation programmes (T2.5). Atos will also lead technical requirements and field deployment of no-gate crossing point solutions (T1.3), (T4.2) and the exploitation roadmap and knowledge transfer (T6.5)</p>
<p>INOV INESC INOVAÇÃO (INOV)</p>
<p>INOV is the leading private non-profit Research and Technology Organisation in Portugal, in the areas of remote detection, ICT and electronics and thus are well placed to lead: technical</p>



verification scanners and smart sensors (T2.2), validation and testing (T2.6), orchestration plan and framework specification (T3.4), development of orchestration framework for no-gate technologies assessment (T3.5), Research data collection and management (T4.3), , Contribution to standards (T6.6.).

Queen Mary, University of London (QMUL)

QMUL is a leading European research centre with extensive expertise in video analytics for the security domain. QMUL will make critical contributions to towards the development of techniques and modules related with video analytics and PERSONA system through leading Study and analysis of latest and new generation no-gate crossing point solutions (T2.1), Video analytics and data fusion for person, object and abnormal behaviour detection (T2.3). As an experienced H2020, and FP7 project coordinator and partner, QMUL are ideally placed to also lead Dissemination, exploitation and liaison with projects lead (WP6), including leading Dissemination planning (T6.1), Dissemination implementation (T6.2), and Liaison with BES-15 and other relevant projects (T6.3).

Swedish Police Authority (SPA)

SPA is the central administrative authority for the police in Sweden, responsible for border control, law enforcement, general social order and public safety within the country. SPA will be a key contributor through leading Use-cases and user requirements (T1.2), and Field deployment planning and preparation (T4.1). SPA will further contribute through: Identification of risks and mitigation controls (T1.6), Research methodology for acceptance assessment (T3.1), Field deployment of no-gate technologies (T4.2), Creation of Advisory Board (T5.1), Creation of network of stakeholders and decision makers (T5.2), Contingency plan and treatment measures (T5.3), Communication of guidelines and best practices to stakeholders (T5.5), and Exploitation roadmap and knowledge transfer (T6.5).

Bundesrechenzentrum – Federal Computing Centre of Austrian Customs (BRZ)

BRZ is the market-leading e-government partner of the federal administration in Austria. The BRZ develops and operates the main federal eGovernment applications, including the applications of the Federal Ministries of Finance and Justice. BRZ will provide key contributions towards Use-cases and user requirements, field deployment of no-gate technologies (T1.2), (T4.1), (T4.2).

Ministry of Interior of the Republic of Serbia (SMOI)

As an LEA SMOI will be a key contributor through participation in and Field deployment (T4.1) (T4.2), and Use-cases and user requirements (T1.2), plus identification of risks and mitigation controls (T1.6), Research methodology for acceptance assessment (T3.1), Creation of Advisory Board (T5.1), Creation of network of stakeholders and decision makers (T5.2), Contingency plan and treatment measures (T5.3), Communication of guidelines and best practices to stakeholders (T5.5), and Exploitation roadmap and knowledge transfer (T6.5).

Ministry of Public Security – Israel National Police (MOPS)

As an LEA MOPS will add their extensive experience to contribute towards Use-cases and user requirements (T1.2), and Field deployment (T4.1) (T4.2). MOPS will also be a valuable contributor towards methodology for acceptance assessment (T3.1), and tasks throughout best practices and communication with stakeholders (WP5) (T5.1), (T5.2), (T5.3), (T5.5), and the future outlook through Exploitation roadmap and knowledge transfer (T6.5).

3.4 Resources to be Committed

The core of the PERSONA project is constituted of technological development, testing and validation and impact creation. The main resources will thus be claimed as personnel cost. In case an action requires additional resources (either effort or cost), the partners have agreed that this will be funded by the responsible partner.

3.4.1 Personnel Effort

The personnel assigned to the various WPs consist of either employee of the companies or potential employees who have already accepted conditional work offers extended by the project partners. Therefore, the risk of not having sufficient manpower needed at each stage is minimal. Additionally, strong interaction and cooperation is deemed necessary during the project's entire life, especially during development of requirements for no-gate crossing technology assessment methodologies, field demonstration and validation.

To achieve the objectives set forth in the project, PERSONA places a special emphasis on the participation of legal research organisations and LEAs for the successful validation of technology assessment. With this objective, the consortium is strongly led by a team of leading legal research organisation (VUB, PRIO) containing several years of expertise in collaborative project participation along with a team of three border control organisation (SPA, BRZ, SMOI, MOPS). As a consequence, a total of 55% of the total effort distribution is allocated to the assessment of technologies while 45% of the total effort is allocated to the technical development team for the development of PERSONA assessment ecosystem. The budget allocated for the technical team also includes the cost required for conducting case-studies with volunteers for the validation of several scenarios envisioned from real-life experiences.

The PERSONA workplan is broadly classified into three categories namely (a) no-gate crossing technology assessment and methodology; (b) technology validation for user acceptance and (c) public outreach and best-practice communication across PERSONA stakeholders. The effort distribution in PERSONA reflects an equal distribution of the overall effort with 32.7%, 31.1 and 29.2% effort distributed for each category respectively.

In particular, each category of effort is split into two WPs to balance the effort distribution among partners in order to complement the partner expertise within the consortium. The overall effort distribution of PERSONA is presented in Figure 12.

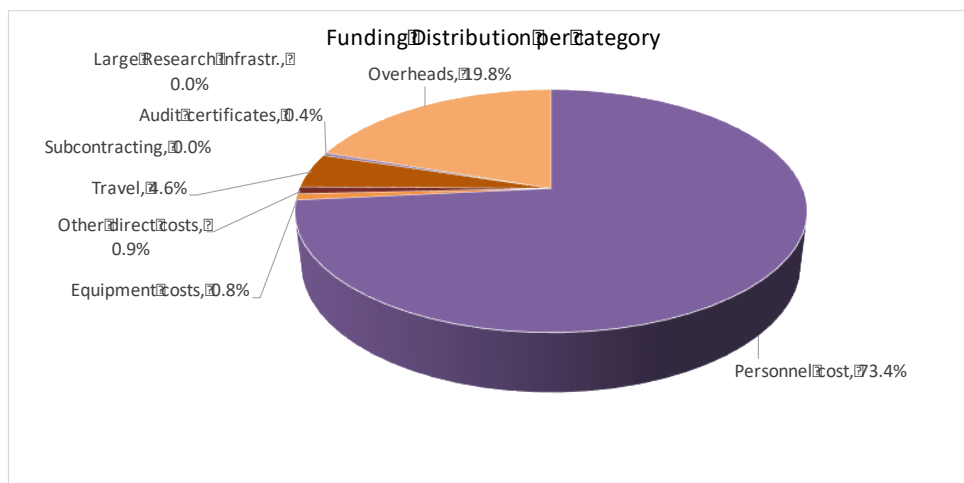


Figure 12 - Effort distribution per workpackage in PERSONA

Regarding the distribution of budget per category as shown in Figure 11, PERSONA will allocate 73.4% of its overall cost to personnel, while only 1.5% is allocated for the other direct cost. This is required to suitably deploy the necessary hardware infrastructure in order to carry out the field trials validating the no-gate crossing technology assessment. The hardware infrastructure procured by INOV will be made available to the consortium for resource sharing. In addition, 0.3% will be allocated as equipment costs to support the consortium partners with necessary infrastructure. This underlines the fact that majority of resources in PERSONA will be used for the development of an assessment ecosystem that brings together legal team, LEAs, industry, research partner and SME to achieve the goals of the project. In this context, 3.9% of the overall cost is allocated to travel in order to mobilise the resources.

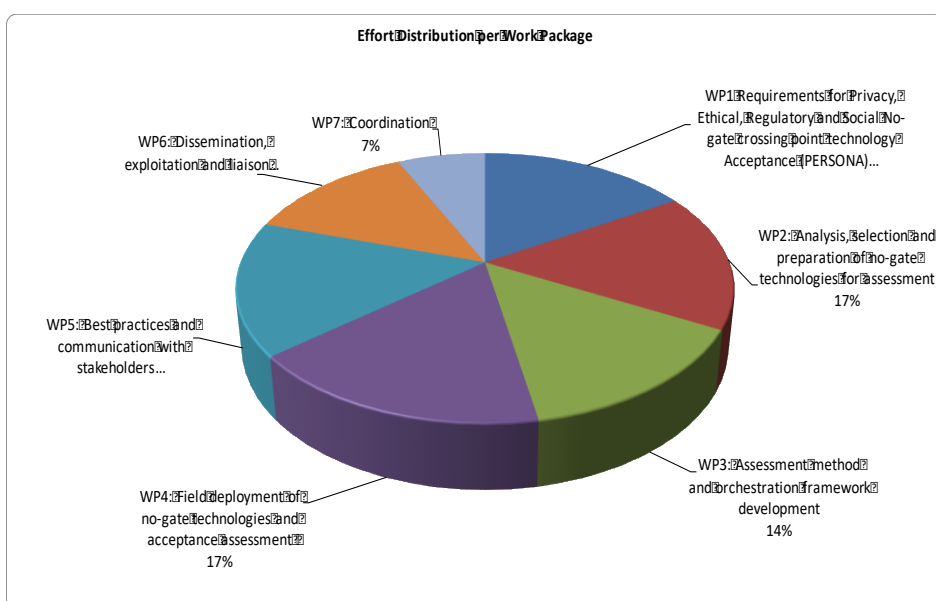


Figure 13 - Overall funding distribution per category in PERSONA

3.4.2 Labour and other direct costs

The overall 'other direct costs' allocated to partners does not exceed the 15%.

3.4.3 Subcontracting

No subcontracting is foreseen. Consortium partners requesting more than €325K have €3000/- for audit certificates.

3.4.4 Resource Mobilisation

PERSONA is primarily driven by legal and ethical partners having 26.7% of the resource allocation with an additional 13.6% allocated to the LEAs. Also, the validation of no-gate crossing technologies will be led by industrial (ATOS) and research partners (QMUL, INOV) with 47.7% of resources allocated. The project partners are highly committed to the projects ambitious objectives and have already committed to mobile resources for achieving the objectives.

3.4.5 Detailed Resources Breakdown



	VUB	PRI0	CEL	ATOS	INOV	QMUL	SPA	BRZ	SMol	MOPS	TOTAL
Personnel	€441 000	€247 000	€248 000	€240 000	€284 200	€390 000	€142 600	€30 400	€56 000	€114 000	€2 193 200
Equipment costs					€25 000						€25 000
Other direct costs	€25 000			€3 000							€28 000
Subcontracting											€0
Travel	€14 000	€15 000	€11 000	€25 000	€14 000	€14 000	€12 000	€8 000	€8 000	€16 000	€137 000
Large Research Infrastr.											€0
Audit certificates											€0
Overheads	€120 000	€65 500	€64 750	€67 000	€80 800	€101 000	€38 650	€9 600	€16 000	€32 500	€595 800
TOTAL COSTS	€600 000	€327 500	€323 750	€335 000	€404 000	€505 000	€193 250	€48 000	€80 000	€162 500	€2 979 000
Total Other direct cost	€39 000	€15 000	€11 000	€28 000	€39 000	€14 000	€12 000	€8 000	€8 000	€16 000	€190 000
FUNDING REQUESTED	€600 000	€327 500	€323 750	€335 000	€404 000	€505 000	€193 250	€48 000	€80 000	€162 500	€2 979 000
percentage of all other costs related to											
personnel costs	8,84%	6,07%	4,44%	11,67%	13,72%	3,59%	8,42%	26,32%	14,29%	14,04%	
Target PMS	60	26	40	50	58	50	23	4	20	19	350
Target Personnel Budg	€ 441 000	€ 247 000	€ 248 000	€ 240 000	€ 284 200	€ 390 000	€ 142 600	€ 30 400	€ 56 000	€ 114 000	€ 2 193 200
TOTAL COSTS (%)	20,1%	11,0%	10,9%	11,2%	13,6%	17,0%	6,5%	1,6%	2,7%	5,5%	100,00%
FUNDING REQUESTED (%)	20,1%	11,0%	10,9%	11,2%	13,6%	17,0%	6,5%	1,6%	2,7%	5,5%	100,00%



Figure 14 - Budget breakdown per partner

4 Members of the Consortium

4.1 Participants (Applicants)

The consortium consists of a carefully selected mix of partners who complement each other with their competencies, experience and ambition at high level. This section provides an overview of the PERSONA partners and their expertise.

4.1.1 Vrije Universiteit Brussel

Partner Number	Partner Full Name	Member State	Partner Type	
1	Vrije Universiteit Brussel	BE	RES	 VRIJE UNIVERSITEIT BRUSSEL
Partner Description				
<p>The multidisciplinary Research Group on Law, Science, Technology & Society (LSTS) was created in 2003 as an independent entity within the Faculty of Law & Criminology at the Vrije Universiteit Brussel (VUB). With more than 35 researchers at all levels of experience, LSTS has become a prominent European research institute in the area of technology regulation. LSTS has a well-established reputation in research concerning privacy and data protection, an area where the work done by LSTS researchers is highly influential. Other research areas at LSTS concern the impact of technologies and surveillance on fundamental rights in the Information Society, Intellectual property rights as they relate to the use of ICTs, the changing nature of law (digital legal theory) and the role of law in relation to science, technology and politics. LSTS researchers operate the Brussels Privacy Hub (www.brusselsprivacyhub.org), an internationally focused privacy research centre and the Privacy Salon, an NGO aiming at public awareness of privacy and other social and ethical consequences of new technologies. As part of the LSTS, researchers also operate the Brussels Laboratory for Data Protection & Privacy Impact Assessments, or d.pia.lab (http://dpialab.brussels), which connects basic, methodological and applied research, provides training and delivers policy advice related to impact assessments in the areas of innovation and technology development. Whilst legal aspects of privacy and personal data protection constitute our core expertise, the Laboratory mobilises other disciplines including ethics, philosophy, surveillance studies and science, technology & society (STS) studies. Predominantly the Laboratory's knowledge and expertise will be utilised in the project. LSTS and its staff have wide experience with conducting research projects of both a basic and an applied nature. To the extent needed, the core team can also draw upon the expertise of further staff members as well as the general resources of the Vrije Universiteit Brussel.</p>				
Key Personnel involved in PERSONA				
<p>Prof. Dr. Paul De Hert (male) is an international fundamental rights expert, with work on human rights and criminal and surveillance law, constitutionalism and the impact of technology on law. He is professor at Vrije Universiteit Brussel (VUB) and associate professor at Tilburg University where he teaches "Privacy and Data Protection" at the Tilburg Institute of Law, Technology, and Society (TILT). At VUB, he holds the chair of 'International, European and Belgian Criminal Law' and 'History of Constitutionalism'. He is Director of the Research Group on Fundamental Rights and Constitutionalism (FRC), Director of the Department of Interdisciplinary Studies of Law</p>				

(Metajuridica) and co-Director of the Research Group Law Science Technology & Society (LSTS). He is member of the editorial boards of several national and international scientific journals.

Dr. Paul Quinn, (male) is a researcher in law and technology and human rights law at the Research Group on Law, Science, Technology, and Society (LSTS). He is active in pursuing a number of his research interests at LSTS, including in areas such as data protection, privacy issues and problems related to stigmatization and discrimination. With respect to the first of these, he has developed an expertise in privacy and data protection issues in the area of health care delivery. He is in particular interested in the evolving use of patient data in health care delivery and has published a number of articles on these issues. In addition, in recent years he has been active a number or European research projects which have a strong focus on these themes. He is also interested on the role of the law in regulating scientific research, an interest that stems from his earlier scientific background.

István Böröcz, LLM (male) is a researcher at the research group on Law, Science, Technology & Society (LSTS). He is a member of the Brussels Laboratory for Data Protection & Privacy Impact Assessments (d.pia.lab). He obtained his LLM in Law and Technology at Tilburg University (2016) and his postgraduate specialist diploma in information and communication technology law at the University of Pécs (2015). He obtained his law degree (JD) at the University of Pécs (2013). His research focuses on the area of privacy and data protection. He is interested in the notion of risk to the rights and freedoms of the individual along with the legal, theoretical and practical issues of the Digital Single Market initiative. He is involved in several EU co-funded research projects, such as MaTHiSiS, FORENSOR, SUCCESS and PARENT. He is a member of the ethical advisory board of the H2020 project CUIDAR (Cultures of Disaster Resilience among children and young people).



Eugenio Mantovani, LLM (male) is a researcher in law and technology and human rights law. He has been involved in several FP7 and H2020 projects where he has been dealing with the ethical, psycho-social and legal, data protection and medical device aspects of technology developments, with particular focus on medical technologies and mobile technologies and on the implications of technology developments on vulnerable groups, such as the elderly. Eugenio is member of the ethical advisory boards of the FP7 project OPSIC (Operationalizing Psychosocial Support in Crisis).

Role in the project

As coordinating partner, VUB will drive the innovation home by leading the management and coordination (WP7), and assessment method and orchestration framework development (WP3). Furthermore, VUB will also lead tasks throughout WP1, WP3, WP4, WP5, and WP6, including: defining requirements (T1.4), user criteria and acceptance (T3.1), (T3.2) and questionnaires and metrics development (T3.3). With a well-established reputation in research concerning privacy and data protection, VUB will also lead privacy, regulatory and data protection acceptance assessment (T4.5), and contribute towards threshold analysis and assessment initiation (T4.4), and social and ethical acceptance assessment (T4.6). In WP5, VUB will lead the contingency plan and treatment measures (T5.3), PERSONA textbook of acceptance (T5.4), and will lead workshop organisation in WP6 (T6.4). VUB will also extensively contribute through participating in analysis of European studies and regulations (T1.1), monitoring of impacts against requirements (T1.5), identification of risks and mitigation controls (T1.6), the creation of Advisory Board (T5.1), communication of guidelines and best practices to stakeholders (T5.5), dissemination and contributions to standards (T6.2), (T6.6).

Output and Background Relevant to the targeted R&D in PERSONA

- KLOZA, D., VAN DIJK, N., GELLERT, R., BÖRÖCZ, I., TANAS, A., MANTOVANI, E., QUINN, P. (Brussels Laboratory for Data Protection & Privacy Impact Assessments (d.pia.lab)), Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals - d.pia.lab Policy Brief No. 1/2017, 2017, ISSN 2565-9936
- VAN DIJK, N., GELLERT, R., ROMMETVEIT, K., A Risk to a Right? Beyond Data Protection Risk Assessments, Journal of Responsible Innovation, September 2014.
- HILDEBRANDT, M., TIELEMANS, L. Data Protection by Design and Technology Neutral Law. Computer Law & Security Review, issue 5, vol.29, 2013, pp.509 - 521.
- WRIGHT D. & DE HERT, P. (Eds.). Privacy Impact Assessment. Dordrecht, Heidelberg, London, New York: Springer, 2012, 523 p.
- GONZALEZ FUSTER G., GUTWIRTH S. (2011) When 'digital borders' meet 'surveilled geographical borders: Why the future of European border management is a problem. In: A Threat Against Europe. Security, Migration and Integration. VUBPRESS, pp. 171-190.

Relevant Previous projects or activities connected to the subject of this proposal


- **MaTHiSiS** (Managing Affective-learning THrough Intelligent atoms and Smart Interactions; **Horizon 2020**) Synopsis: The MaTHiSiS learning vision is to provide a product-system for vocational training and mainstream education for both individuals with an intellectual disability and non-diagnosed ones. This product-system consists of an integrated platform, along with a set of re-usable learning components (educational material, digital educational artefacts etc.), which will respond to the needs of a future educational framework, as drawn by the call, and provide capabilities for: i) adaptive learning, ii) automatic feedback, iii) automatic assessment of learner's progress and behavioural state, iv) affective learning and v) game-based learning. To achieve these educational innovative goals, the MaTHiSiS project will introduce a novel methodology in the education process. The so-called learning graphs which, acting as a novel educational structural tool and associated with specific learning goals, will foster novel ways to guide how the different learning material and artefacts can be deployed throughout a prespecified learning scenario. The building materials of these graphs are drawn from a set of Smart Learning Atoms (SLAs) which will constitute the vertices of the graphs. SLAs are learning elements that carry stand-alone pieces of learning materials, targeting certain problems. More than one SLAs, working together on the same graph, will be able to help individuals reach their learning/training goals. The learning goals as well as the SLAs involved will be decided and pre-agreed based on common practices, goals derived from formal and non-formal education (general education, vocational training, lifelong training or specific skills learning) as well as learner's own goals (so as to equally serve in-formal education contexts). The MaTHiSiS consortium is coordinated by Atos Spain and consists of 18 beneficiary organizations from 9 different Member States collaborating, namely Spain, France, Greece, UK, Netherlands, Belgium, Italy, Lithuania and Germany. <http://www.mathisis-project.eu>
- **FORENSOR** FOREnsic evidence gathering autonomous seNSOR; **Horizon 2020** Synopsis: Covert evidence gathering has not seen major changes in decades. Law enforcement Agencies (LEAs) are still using conventional, manpower-based techniques to gather forensic evidence. Concealed surveillance devices can provide irrefutable evidences, but current video surveillance systems are usually bulky and complicated, are often used as simple video recorders, and require complex, expensive infrastructure to supply power, bandwidth, storage and illumination. Recent years have seen significant advances in the surveillance

industry, but these were rarely targeted to forensic applications. The imaging community is fixated on cameras for mobile phones, where the figures of merit are resolution, image quality, and low profile. A mobile phone with its camera on would consume its battery in under two hours. Industrial surveillance cameras are even more power hungry, while intelligent algorithms such as face detection often require extremely high processing power, such as backend server farms, and are not available in conventional surveillance systems. Here we propose to develop and validate a novel, ultralow- power, intelligent, miniaturised, low-cost, wireless, autonomous sensor ("FORENSOR") for evidence gathering. Its ultra-sensitive camera and built-in intelligence will allow it to operate at remote locations, automatically identify pre-defined criminal events, and alert LEAs in real time while providing and storing the relevant video, location and timing evidence. FORENSOR will be able to operate for up to two months with no additional infrastructure. It will be manageable remotely, preserve the availability and the integrity of the collected evidence, and comply with all legal and ethical standards, in particular those related to privacy and personal data protection. The combination of built-in intelligence with ultra-low power consumption could help LEAs take the next step in fighting severe crime. <http://forensor-project.eu/>

- **EPINET** Integrated Assessment of Societal Impacts of Emerging Science and Technology from within Epistemic Networks (**FP7**). Synopsis: The EPINET project introduces a new approach to promote integration of technology assessment (TA) methods. It will develop methods and criteria to be used for more socially robust and efficient practices on the interfaces between TA and the world of policy makers and innovators. EPINET introduces the concept of epistemic networks as a way of conceptualising complex developments within emerging fields of sociotechnical innovation practices. It establishes a "soft" framework within which the plurality of different TA practices can be explored in a concerted manner. Four cases are investigated along with the development of this framework: wearable sensors, cognition for technical systems, synthetic meat and smart grids. "Integrating TA", it is claimed, is a task for empirical investigation in which implicit values of TA methodologies, disciplines and practices are spelled out and placed in relation to the practices they are meant to assess. EPINET develops a framework for integrating assessments through gradual co-production of methodologies and concepts (centrally that of "responsible innovation") together with innovators and policy makers. The challenges of "integrating assessments", we claim, can only be gradually worked out within such a holistic view of complex intersecting networks and practices. <http://www.epinet.no/>
- **PIAF** A Privacy Impact Assessment Framework for data protection and privacy rights; JUST/2010/FRAC/AG/1137 30-CE-0377117/00-70; January 2011 – October 2012 Synopsis: PIAF was a European Commission co-funded research Project that aims to encourage the EU and its Member States to adopt a progressive privacy impact assessment policy as a means of addressing needs and challenges related to privacy and to the processing of personal data. The 22-month project included, in its first phase, a review of privacy impact assessment policies and practices in Australia, Canada, Hong Kong, Ireland, New Zealand, the US and UK to identify which elements may be used effectively to construct a model framework applicable to the EU. <http://piafproject.eu>
- **ADVISE** Advanced Video Surveillance archives search engine for security applications; **FP7-SEC-2011-285024**; 2012-2015. ADVISE is a research project aimed at designing and developing a unification framework for surveillance-footage archive systems. The ADVISE project results eases the work of law enforcement authorities in their fight against crime and terrorism, through negotiation of all relevant legal, ethical and privacy constraints, and through location-based video archive selection and efficient evidence mining of multiple, heterogeneous video archives. In a context where surveillance systems are continuously growing in scale,

heterogeneity and capabilities, two major obstacles have to be overcome. On the one hand, the variety of technical components of surveillance systems, producing video repositories with different compression formats, indexing systems, data storage formats sources, has to be addressed. On the other hand, the legal, ethical and privacy rules that govern surveillance and the produced content have to be taken into account. To address these two major issues, the ADVISE system is composed by two major components: the first one performing the semantically enriched, event-based video analysis which offer efficient search capabilities of video archives and sophisticated result visualization, and the second one enforcing the legal, ethical and privacy constraints that apply to the exchange and processing of surveillance data. Within ADVISE, the VUB study team is responsible for the development and implementation of the legal, ethical and privacy impact assessments. <http://www.advise-project.eu/>.

4.1.2 Peace Research Institute Oslo (PRIO)

Partner Number	Partner Full Name	Member State	Partner Type	
2	Institut for Fredsforskning Stiftelse Peace Research Institute Oslo	NO	RES	

Partner Description

Established in 1959, PRIO is a key institution within peace research with a primary mission to conduct high-quality academic research on conditions for peaceful relations between states, groups and people. PRIO is an independent and international institute located in central Oslo, housing several thematic research groups. Within PRIO, the Security Research Group has been coordinator of three FP7 projects and partner in eight other projects dealing with various security topics, such as societal security, ethical and rights-related dimensions of security policies, privacy and personal data protection, crisis management and resilience. The researchers in the Security Research Group come from diverse disciplinary backgrounds, such as political science, international relations, law, sociology, war and peace studies, philosophy, cultural studies, and criminology. Methodologically, the group focuses on qualitative research such as interviews, document analyses and case studies. It also has also developed methodologies to integrate ethical, rights-related and other aspects of societal security into the development of tools for security governance. The group takes a critical approach to security, drawing on governmentality studies and genealogy, conceptual and cultural history, political philosophy, media studies, and social theory, and endorsing self-reflective and non-Euro-centric perspectives.

Key Personnel involved in PERSONA

Dr. Maria Gabrielsen Jumbert (female) is a senior researcher and director of the Dimensions of Security department at the Peace Research Institute Oslo (PRIO). She also leads the Norwegian Centre for Humanitarian Studies (NCHS). Her research focuses on EU border security policies in the Mediterranean (competing narratives on migration, humanitarian needs and border control) and on security and humanitarian surveillance technologies. She conducted research on the legal, ethical and political aspects of EU maritime border surveillance in the FP7 project PERSEUS.



She leads two collaborative research projects funded by the Norwegian Research Council, on the topics of humanitarianism and digital risk communication.

Dariusz (Darek) Kloza, LL.M (male) is a full-time researcher with the Research Group on Law, Science, Technology and Society (LSTS) at Vrije Universiteit Brussel (VUB) and part-time with the Peace Research Institute Oslo (PRIO). He also freelances at the Centre for Direct Democracy Studies (CDDS) at University of Białystok. His expertise concentrates on the governance of privacy and personal data protection, in particular on the notion of impact assessments for emerging technologies. He is a founding member of the Brussels Laboratory for Data Protection & Privacy Impact Assessments (d.pia.lab) at VUB-LSTS. He has been involved in a number of EU co-funded research projects, such as PIAF, ADVISE, EPINET, LASIE, FORENSOR, PARENT and MATHISIS. He holds both an LL.M. in Law and Technology (2010) from the Tilburg Institute for Law, Technology, and Society (TILT) at Tilburg University (with distinction) and a master’s degree in law from the University of Białystok (2008), having also studied at the University of Copenhagen (2007-2008).



Stine Bergersen (female) is a researcher at the Peace Research Institute Oslo (PRIO), where she coordinates the Security Research Group. Her research interest includes risk communication and terrorism, privacy and personal data protection, practices of surveillance, and innovation in European crisis management. She graduated in 2012 with master’s degree in criminology from University of Oslo.



Role in the project

PRIO is a key institution within peace research with a primary mission to conduct high-quality academic research on conditions for peaceful relations between states, groups and people. PRIO, the Security Research Group coordinated 3 FP7 projects and partnered in 8 other projects dealing with various security topics, such as societal security, ethical and rights-related dimensions of security policies, privacy and personal data protection, crisis management and resilience. PRIO’s vast experience will be facilitate achieving PERSONA outcomes through leading requirements for privacy, ethical, regulatory and social no-gate crossing point technology acceptance (PERSONA) (WP1), including leading analysis of EU studies and regulations (T1.1), monitoring of impacts against PERSONA requirements (T1.5), identification of risks and mitigation controls (T1.6). PRIO will also lead field deployment of no-gate technologies and acceptance assessment (WP4), including threshold analysis and assessment initiation (T4.4), social and ethical acceptance assessment (T4.6), and participating in privacy, regulatory and data protection acceptance assessment (T4.5). Further contributions will be made through: research methodology for acceptance assessment (T3.1), criteria for user perception analysis (T3.2), questionnaires and metrics development (T3.3), the creation of the Advisory Board, network of stakeholders and decision makers, contingency plan and textbook of acceptance (T5.1) (T5.2), (T5.3) (T5.4).

Output and Background Relevant to the targeted R&D in PERSONA


- Jumbert Gabrielsen Maria (2012) ‘Controlling the Mediterranean Space Through Surveillance: The Politics and Discourse of Surveillance as an All-encompassing Solution to EU Maritime Border Management Issues’, *Espace, Populations, Sociétés*, 3: 35-48.
- Kloza Dariusz, Niels van Dijk, and Paul De Hert (2015) “Assessing the European Approach to Privacy and Data Protection in Smart Grids. Lessons for Emerging Technologies” in *Smart Grid Security. Innovative Solutions for a Modernized Grid*, Florian Skopik (Ed.), Elsevier.

- Wright, David; Rowena Rodrigues; Charles Raab; Richard Jones; Ivan Szekely; Kirstie Ball; Rocco Bellanova and Stine Bergersen (2015) ‘Questioning Surveillance’, Computer Law & Security Review 31(2): 280–292.
- Bergtora Sandvik Kristin and Maria Gabrielsen Jumbert, eds, (2016) The Good Drone. New York: Routledge.
- Kloza Dariusz, Niels van Dijk, Raphaël Gellert, István Böröcz, Alessia Tanas, Eugenio Mantovani and Paul Quinn (2017) Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals, d.pia.lab [Brussels Laboratory for Data Protection & Privacy Impact Assessments (d.pia.lab)] Policy Brief No. 1/2017, Brussels.

Relevant Previous projects or activities connected to the subject of this proposal

- FP7 SEC-2010.3.1-1 **PERSEUS** “Protection of European seas and borders through the intelligent use of surveillance” (Partner)
- FP7 SEC-2011.5.1-2 **IRISS** “Increasing Resilience in Surveillance Societies” (Partner)
- FP7 SEC-2010.6.3-3 **DESSI** “Decision Support on Security Investment” (Partner)
- FP7 SEC-2011.6.5-2 **PACT** “Public perception of security and privacy” (Scientific Coordinator)
- FP7 SEC-2013.1.6-1 **LASIE** “LArge Scale Information Exploitation of Forensic Data” (Partner)

4.1.3 Cyberethics Lab

Partner Number	Partner Full Name	Member State	Partner Type	
3	Cyberethics Lab	IT	SME	

Partner Description

CEL is a start-up Italian SME leveraging on the experience and knowledge of its multidisciplinary core members, teaching at the University and working in numerous R&D activities in the context of inter-disciplinary EC Research projects. CEL’s main focus is a holistic vision of innovation, generated by efficiency, scientific curiosity and respect for human beings, where ideas, techniques, tools and methods from different disciplines are integrated to make innovative, secure and responsible technology. CEL offering is mainly based on promoting innovation as well as creating ethical awareness and promoting ethical behaviour to build confidence and trust, as well as the promotion of the inclusion of legal and ethical concerns in the design and implementation of technologies, the identification of risks on individual fundamental rights and the issuing of recommendations in order to make technologies compliant with ethical principles and the current legal framework.

Key Personnel involved in PERSONA

Prof. Teresa Numerico (female) is associate professor in Philosophy of Science at the Department of Philosophy, communication and performing arts (University of Rome III) where she teaches courses on network communication and history and philosophy of computer science and Technology since 2008. She has an experience of fifteen years in the field of philosophy and history and ethics of computer science and artificial intelligence and has been lecturing on these subjects in Italy and abroad since 2001. After a PhD in history of science in which she was based

between Rome, Bari and London (1994-1998), she worked for almost four years as a manager in two media companies: Sky and the Italian branch of Turner company, during the merge between AOL and Time Warner, where she was head of the new born digital marketing area and later head of business development of new digital products of Turner company. Between 2001 and 2003 she was awarded a post-PhD Fellowship at the University of Salerno, and after she was awarded a Leverhulme Trust Research Fellowship in 2004-2005. Between 2005 and 2008 she was lecturer at the university of Salerno, where she taught courses in web design and theory and techniques of the new media. Her research interests range from philosophy of computer science and digital humanities to social informatics, from ethics to politics of telecommunication technologies.

Dr Letícia Duboc (female) is an Honorary Research Fellow at the Computer Science Department at the University of Birmingham, UK. She holds a PhD on Computer Science from the University College London (UCL), in the UK, as well as a master and a bachelor's degree in computer science from the Federal University of Rio de Janeiro (UFRJ), in Brazil. Her work focuses on sustainability in systems engineering. She is part of an international consortium of researches (sustainabilitydesign.org) aiming to raise awareness of technology designers about their responsibility with respect to the long-term consequences of their designs and to provide technical solutions that with help them to do so. She is author of several articles and she has been involved in different EU projects, as responsible of the ethical impact assessment of technology.



Role in the project

CEL will contribute to the project supporting the promotion of the project innovation and project's outcomes uptake on the market. CEL will also participate in the project activities related to the assessment of ethical and legal concerns. CEL is a start-up Italian SME leveraging on the experience and knowledge of its multidisciplinary core members, teaching at a University and working in numerous R&D activities in the context of inter-disciplinary EC Research projects. CEL are thus well equipped to lead, best practices and communication with stakeholders (WP5) including the creation of the Advisory Board (T5.1), creation of network of stakeholders and decision makers (T5.2), and communication of guidelines and best practices to stakeholders (T5.5). CEL will further contribute their legal and ethical awareness expertise through participating in tasks throughout WP1: analysis of EU studies and regulations (T1.1), definition of requirements (T1.4), and monitoring of impacts against PERSONA requirements (T1.5), threshold analysis and assessment initiation (T4.4), privacy, regulatory and data protection acceptance assessment (T4.5), social and ethical acceptance assessment (T4.6). Further contributions will include user assessment, perception and metrics development (T3.1), (T3.2), (T3.3), contingency plan and treatment measures (T5.3), PERSONA textbook of acceptance (T5.4), dissemination, workshop organisation, and exploitation roadmap (T6.1) (T6.4) (T6.5).

Output and Background Relevant to the targeted R&D in PERSONA

- Numerico T., Fiormonte D., Tomasi F., a volume in *The digital humanist: a critical Inquiry*, Punctum Books, Brooklyn, 2015
- Numerico T., "Social networks and web minorities", in *Cognitive Systems Research*, Vol. 4, Issue 4, pp. 355-364, 2003
- Numerico T., "The New Machine: From Logic To Organization. Turing, Von Neumann And A Self-Organized Device For Future Applications", Rutherford Journal, 2010
- Numerico T., Cordeschi R., "Dalla cibernetica a Internet: etica e politica tra mondo reale e mondo virtuale" in *Il Corpo Post-Umano. Scienza Diritto Società*, Carocci Editore, 2012

<ul style="list-style-type: none"> Numerico T., “Filosofia e Diritto nell’era di Internet”, in <i>Filosofia E Diritto Nell’Era Di Internet</i>, pp. 85-105, 2002
Relevant Previous projects or activities connected to the subject of this proposal
<p>Listed projects have been participated by the company core members engaged in numerous R&D activities in the context of inter-disciplinary research projects.</p> <ul style="list-style-type: none"> ADVISE - <i>Advanced Video Surveillance archives search Engine for security applications</i> – FP7- Security Workprogramme of the European Commission - http://www.advise-project.eu/. Role: promotion of the Privacy by Design methodology through the Privacy Impact Assessment framework. ABC4EU – <i>Automated Border Control Gates for Europe</i> - http://abc4eu.com/. Role: implementation of the Ethical, Legal and Social Impact Assessment of the research process and the technology implemented by the project. <i>Modelli e interferenze nella Scienza</i>, PRIN Project (National funding), 2014. S.F.B.F.: <i>space for building the future</i>, POR FSE Campania 2014/2020 – <i>Benessere giovani Organizziamoci</i>. Role: implementation of educational and cultural laboratories on the ethical use of technologies; dissemination of project results. <i>Scuola e famiglia Respons-Agile</i>, PON FSE MIUR 2016-2017 - <i>Inclusione sociale e lotta al disagio</i>. Role: implementation of educational and cultural laboratories on the ethical use of technologies; dissemination of project results.

4.1.4 Atos

Partner Number	Partner Full Name	Member State	Partner Type	
4	Atos	ES	IND	
Partner Description				
<p>Atos is a global leader in digital transformation with approximately 100,000 employees in 72 countries and annual revenue of around € 12 billion. The European number one in Big Data, Cybersecurity, High Performance Computing and Digital Workplace, The Group provides Cloud services, Infrastructure & Data Management, Business & Platform solutions, as well as transactional services through Worldline, the European leader in the payment industry. With its cutting-edge technologies, digital expertise and industry knowledge, Atos supports the digital transformation of its clients across various business sectors: Defense, Financial Services, Health, Manufacturing, Media, Energy & Utilities, Public sector, Retail, Telecommunications and Transportation.</p> <p>The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, Unify and Worldline. Atos SE (Societas Europaea) is listed on the CAC40 Paris stock index.</p> <p>Atos Research & Innovation (ARI) is the R&D hub for emerging technologies and a key reference for the whole Atos group. With almost 30 years of experience in running Research, Development and Innovation projects, we have become a well-known player in the EU context. Our</p>				



multidisciplinary and multicultural team has the skills to cover all the activities needed to run projects successfully, from scientific leadership to partnership coordination, from development of emerging technologies to the exploitation of project outcomes, with a strong focus on dissemination, innovation adoption and commercialization.

The Homeland and Security Defence Sector within the Atos unit of Research & Innovation coordinates the R&I activities in the security sector, based on experience gained with clients that include national and regional security bodies, intelligence agencies, international bodies (such as the UN, NATO and the EU) and also all types of organizations that address or deal with citizen safety, critical infrastructures, crisis management, crime fighting, law enforcement or border intelligence. The key strengths and special areas of experience span from crisis and emergency management to cross border management and interoperability, simulation of forward-looking security scenarios, economics of security or security societal issues. The team of experts of the HSD Sector has been performing essential security and crisis management projects for many years (e.g. DRIVER, ZONESEC, PACT, VALUESEC, CIRAS, FORCE, RECOBIA, FOCUS, VIRTUOSO, ZONESEC, etc.) aiming to close the gaps between technology, IT and the society security related needs and challenges.

Key Personnel involved in PERSONA

Jaime Martín (male) is Deputy Head of the Homeland Security and Defence Sector of the Research and Innovation group of Atos. He has strong managerial and technical skills which he has proven in European research projects in the scope of security. His expertise covers critical infrastructures, decision support systems, crisis management, society resilience, risk analysis, eID and privacy. He has experience managing consortia teams across different countries as both project manager and technical coordinator in charge of definition of requirements, functional and technical design, use cases definition, development, integration, testing, dissemination and exploitation. As senior researcher he has been editor and main contributor of many technical deliverables of the European Commission in the scope of security. Jaime has also experience as speaker in international symposia and conferences and as chairman in international research workshops. Jaime holds a Msc degree in Computer Science Engineering from the Universidad de Deusto, Spain

Jose-Ramon Martinez-Salio (male) is currently technical manager for HSD projects and technological specialist in ATOS. He has a degree in Industrial Engineering from the Universidad Politecnica de Madrid. In Atos he works in the Homeland and Security Defence Sector that is part of the Atos Research & Innovation department. He has been involved as technical manager in several research projects like CIRAS (Critical Infrastructure Risk Assessment Support) and ZONESEC (EU framework for the security of widezones). Jose-Ramon has a strong technical background in software development teams, software architecture and R&D, team management and coordination. Jose-Ramon has a solid expertise in international team coordination and a long-time experience in NATO groups and in international standardization organizations like SISO.

Mr Ross Little (male) is a project manager in the Identity and Privacy Lab under Atos Research & Innovation. He has been involved in many of the labs security-related national and European projects (which include IDENTICA, Segur@, Thofu, PICOS, SEMIRAMIS, MobiGuide, DAPHNE, MoveUS, STORK, STORK 2.0, STRATEGIC, FutureID and ABC4EU). He has a long background in data and telecommunication protocols and systems. He is experienced in LSP coordination in STORK 2.0 and in providing Privacy and Security by Design in ICT cloud deployments in several EU projects, so to ensure EU data protection compliance in the protection of personal and sensitive data. Current activities include leading a team of developers in the development of fixed and



mobile smart border biometric systems in ABC4EU. He holds a B.Eng degree in Electrical and Electronic Engineering (E.E.E) at the University of Strathclyde.


Role in the project

As a global leader in digital transformation with cutting-edge technologies, digital expertise and industry knowledge, Atos supports the digital transformation of its clients across various business sectors: Defense, Financial Services, Health, Manufacturing, Media, Energy & Utilities, Public sector, Retail, Telecommunications and Transportation. Atos are thus ideally positioned to lead the analysis, selection and preparation of no-gate technologies for assessment (WP2), including contributing towards all WP2 tasks, and specifically leading verification scanners and smart sensors (T2.2), security assessment and decision support systems (T2.4), systems for facilitation programmes (T2.5). Atos will also lead technical requirements and field deployment of no-gate crossing point solutions (T1.3), (T4.2). Additional key contributions will be made towards: Identification of risks and mitigation controls (T1.6), orchestration plan and framework specification (T3.4), development of orchestration framework for no-gate technologies assessment (T3.5), Field deployment planning and preparation (T4.1),c of network of stakeholders and decision makers (T5.2), communication of guidelines and best practices to stakeholders (T5.5), liaison with BES-15 and other relevant projects (T6.3), exploitation roadmap and knowledge transfer (T6.5), and contribution to standards (T6.6).

Relevant Previous projects or activities connected to the subject of this proposal

- **ABC4EU:** stands for Automated Border Control Gates for Europe. It is part of the Seventh Framework Program for Research, Technological Development and Innovation of the European Union, started in 2014 and to be completed in 2018. Its main objective is to standardize automated border control systems (ABCs) and integrate these systems with the new EES (Entry and Exit System) and NFP (National Facilitation Programs), as proposed in the Smart Borders Package European Union. <http://abc4eu.com/>
- **CIRAS:** fills an existing gap in Critical Infrastructure Protection. The new approach presented by CIRAS results from the methodology and tools elaborated during **FP7 ValueSec** project. These tools facilitate the evaluation of security measures and support the decision maker in deciding on concrete measures with maximum overall benefit. This selection of security measures is based on three tool “pillars”: the risk reduction capability of the measure, its costs-benefits relation, and the assessment of the various restrictions and qualitative factors of influence (political, legal, societal, etc.). <http://cirasproject.eu/content/project-topic>
- **VALUESEC:** The task of VALUESEC is defining, context modeling, weighting and quantifying attributes of costs and benefits, advantages and disadvantages of security measures, and demonstration of an application tool evaluating the different effects and the aggregated value of security measures. <http://www.valuesec.eu/>

4.1.5 INOV INESC INOVAÇÃO

Partner Number	Partner Full Name	Member State	Partner Type	
5	Inov	PT	IND	

Partner Description

INOV INESC INOVAÇÃO is the leading private non-profit Research and Technology Organisation in Portugal, in the areas of remote detection, ICT and electronics. The INOV mission is to lead technological development and innovation processes, in close cooperation with governments, enterprises and universities. INOV has accumulated strong technical expertise in: monitoring and surveillance solutions; communications; complex systems integration and analysis; electronics product development; artificial intelligence; cyber security & defence; enterprise engineering & IT governance; social engineering; risk and resilience management for critical infrastructures (CI).

Based on this experience, INOV is focused on doing applied research and providing engineering and consultancy services, as well as planning, assessment and coordination of end-user driven National and European R&D projects, with over 70 participations in the last 10 years. INOV also possesses wide experience in organisation of demonstration tests and field experiments with large number of participants (incl. LEAs), related to security, surveillance, and risk management. INOV has consolidated knowledge and proven installed solutions for monitoring with subsequent data fusion, with clients and partners worldwide.

It is also important to mention that INOV has National, European and North Atlantic Treaty Organization (NATO) security clearance. As board member of DANOTEC (Association of Defense Business, Weaponry and New Technologies) and associated partner at AFCEA (Association for Communications, Electronics, Intelligence and Information Systems for National Defence), INOV actively exchanges knowledge and coordinates R&D activities to respond to current and emerging defence and security challenges.

Key Personnel involved in PERSONA

Tiago Rocha da Silva (male), graduated in Electrical Engineering at the Instituto Superior Técnico, Lisboa, Portugal in 1986. He also acquired an M.Sc. degree in Electronics Engineer and Computers, Telecommunication profile, in 1993 at the same institute. Presently he is Coordinator of Telecommunications Systems & Technologies Unit. He has been involved in many research activities in the area of Telecommunications since 1986 also experience in Wireless Sensor and Actor Networks and Navigation systems, participated in European (H2020: ROCSAFE(SEC-700264), TRILLION(SEC-653256); FP7: SIIP(SEC-607784), TASS(SEC-241905), HANDHOLD(SEC-284486), , WSAN4CIP(ICT-225186), LOCON(ICT-224148), AAS(TRANSPORT-213061); FP6: AIRNET(IST-507888), SENSATION(IST-507231); Eureka: SECAIR(6030); EXPLOIT-IWU ATM-2Mbit/ISDN and RACE: "Technology for ATD-TA), ESA Projects (Early Trials, ARMAS, GAMMA) and National projects. He is a telecommunication expert, with more than twenty years of experience involved not only on system development but as well on consulting and advice for different sectors, including Public Sector, Telecom Operators, Utilities, bank and Health sectors.

Filipa Borrego (female) is the Innovation Management Coordinator and also Senior Researcher at INOV. Her research focus is on system architecture, targeting high performance and/or low power computing. Filipa graduated in Electronics and Telecommunications Engineering at the University of Aveiro, Portugal, and has a Ph.D. in Computer Architecture at Delft University of Technology, the Netherlands. She was a trainee at the European Space Agency (ESA) and a researcher at Holst Centre / IMEC, the Netherlands. She was also a Portuguese National Contact Point for the Security theme of the European Framework Programme Horizon 2020 (H2020) and a Portuguese National Expert for the Committee of Information and Communication Technologies (ICT) of H2020. Filipa was a Fulbright Visiting Scholar at the University of Texas, Austin, USA,



working on methodologies to develop, license and/or commercialize early-stage technologies coming out of European projects.

Paulo Chaves (male) has 2 degrees in Electric Engineering and is a R&D senior specialist at INOV, with an extensive experience in involvement and coordination (project management) of national, EU and ESA projects (since 1999). He also possesses experience in remote monitoring systems, signal processing, navigation systems, sensor fusion for security and transportation applications. He is responsible of the area of electronics and monitoring system at INOV. He has large experience in product development for monitoring systems. He has delivered 15 communications to national and international conferences and regularly collaborates with several national and international organizations as a technology consultant.

John Rodrigues (male) is a head of the Security & Defence Business Unit at INOV, as well as member of the Board of Director of the Portuguese Association of Security & Defence Industries (DANOTEC). He has a degree in electronics and computer science (1994), Technical University of Lisbon) and certificates of several security courses, including Industrial Security Course from the Portuguese National Security Office (2009); Advanced Course for Security Directors from the United Nations Interregional Crime and Justice Research Institute (2011); Counter-Terrorism Intensive Course from the Portuguese Institute of Police Sciences and Internal Security (2013). With more than 18 years' experience as consultant and project manager, he possesses extensive knowledge on safety and security for critical infrastructures. He has participated in 11 FP7 / H2020 Security projects, as well as many other security related projects and studies for national and international entities, including NATO and the Portuguese Government.

Role in the project

Inov is the leading private non-profit Research and Technology Organisation in Portugal, in the areas of remote detection, ICT and electronics and thus are well placed to lead: technical validation and testing (T2.6), orchestration plan and framework specification (T3.4), development of orchestration framework for no-gate technologies assessment (T3.5), Research data collection and management (T4.3), Exploitation roadmap and knowledge transfer (T6.5), Contribution to standards (T6.6). Valuable contributions will also be made through participating in all tasks in Analysis, selection and preparation of no-gate technologies for assessment technical requirements of no-gate crossing point solutions (WP2), plus analysis, selection and preparation of no-gate technologies for assessment (T1.3), Identification of risks and mitigation controls (T1.6), Field deployment planning and preparation, and deployment (T4.1)(T4.2), Contingency plan and treatment measures (T5.3), Communication of guidelines and best practices to stakeholders (T5.5), plus Liaison with BES-15 and other relevant projects (T6.3).

Output and Background Relevant to the targeted R&D in PERSONA

- SAFEGROUND™, an A-SMGCS system (Advanced -Surface Movement Guidance and Control System) , which helps manage and control all airport vehicles (utility vehicles, catering , baggage, fuel, maintenance, fire service, police, customs) in coordination with the monitoring aircraft, implementing the ICAO and EUROCONTROL recommendations for such systems: geographic information according to WGS84 and stratified Cartography in themed levels in accordance with the ED -119 (EUROCAE- Common Database Interchange Standard for Terrain, obstacle and Aerodrome Mapping Data - based on ISO 19100). The system main target are airfields, small and medium-sized airports and can be used as a complementary system in large airports. The system was developed in collaboration with ANA (Aeroporos de Portugal),

to improve safety and airport movement areas (runways, taxiways and apron), improves the safety services provide continuity of service, integrity and efficiency of operations specially in low visibility, crisis and emergency situations and also full airport data integration and provide decision support services.

- CICLOPE™ is a surveillance system designed by a team of INOV researchers, highly experienced in development of monitoring and remote-control systems. The CICLOPE system currently covers about 1,300,000 hectares of Continental Portugal. Due to characteristics of its equipment, CICLOPE enables large areas to be monitored remotely, at a reduced cost per hectare. The simultaneous or individual use of video and IR cameras, as well as a special lidar (laser radar) sensor, allows round-the-clock observations, practically regardless of the weather conditions. With completely autonomous power supply and communications units, the CICLOPE system is designed to operate in any location. The cameras and all the associated equipment (e.g. sensors), including the positioning and control systems are installed in the special observation towers called SDATs (Surveillance and Data Acquisition Towers).

Relevant Previous projects or activities connected to the subject of this proposal

- **TASS** (FP7-Security 241905 - 2010/2014), TASS is a multi-segment, multi-level intelligence and surveillance system, aimed at creating an entire airport security monitoring solution providing real-time accurate situational awareness to airport authorities. The TASS concept is based on integrating different types of selected real-time sensors & sub-systems for data collection in a variety of modes, including fixed and mobile, all suitable for operation under any environmental conditions.
- H2020-DS-653618: **DOGANA** “Advanced Social Engineering and Vulnerability Assessment Framework”, www.dogana-project.eu, is an IA that directly addresses the complexity stemming from the human dimension of attacks and aims to deliver solutions to help enterprises manage the risks associated with social engineering. Being directly mentioned by the European Commission in the Call description, human factor should be taken into consideration in any security related investigation.
- H2020-SEC-700264: **ROCSAFE** “Remotely Operated CBRNe Scene Assessment Forensic Examination”, with the goal of fundamentally change how CBRNe events are assessed, in order to and ensure the safety of crime scene investigators by reducing the need for them to enter high-risk scenes when they have to determine the nature of threats and gather forensics.
- H2020-FCT-700381: **ASGARD** “Analysis System for Gathered Raw Data”, with the goal to contribute to Law Enforcement Agencies Technological Autonomy effectively use the technology. Technologies are to be transferred to end users under an open source scheme focusing on Forensics, Intelligence and Foresight (Intelligence led prevention and anticipation).
- FP7-SEC-261605: **SECUR-ED** “Secured Urban Transportation – European Demonstration”, www.secured.eu, was a demonstration project with an objective to provide a set of tools to improve urban transport security. The list of participants included all major stakeholders from Europe. SECUR-ED was one of the most representative forums in which European transportation operators, authorities, academia and industry openly discussed cyber security in public transportation systems.
- FP7-SEC-607784: **SIIP** “Speaker Identification Integrated Project”, <http://www.siip.eu>, SIIP research project is developing a break-through Suspect Identification solution based on a novel Speaker Identification (SID) engine and Global Info Sharing Mechanism (GISM) which will identify unknown speakers that are captured in lawfully intercepted calls, in recorded

crime or terror arenas and in any other type of speech medium and channel (including social-media).

Significant infrastructure and/or any major items of technical equipment that's relevant to the proposed work


Computer centre, which possesses teraflop-scale computers based on the most contemporary GPGPU technology (processors NVIDIA Tesla K20) and corresponding software (CUDA SDK, Matlab, etc.).

Development Laboratories: these premises are provided with a wide range of supporting equipment, including components (electronic and conventional SMD, wires, cables, connectors, bolts, and so on), diverse tools, gauges and electronic devices (power supplies, function generators, multimeters, oscilloscopes, analysers and programming hardware).

Testing facilities: a special room designated to tests on robustness of the developed equipment, including environmental and electromagnetic compatibility (for pre-certification). The facilities include an "oven" (temperature/humidity control), a "bathtub" with shower and closed water circulation, and UV lamps (used for water and solar radiation resistance tests of equipment).

Special conference rooms with all technical infrastructure requirements to support periodic meetings and the realization of workshops.

4.1.6 Queen Mary University of London (QMUL)

Partner Number	Partner Full Name	Member State	Partner Type	
6	Queen Mary, University of London	UK	RES	

Partner Description

Queen Mary, University of London (QMUL) is one of the UK's leading research-focused higher education institutions. Amongst the largest of the colleges of the University of London, QMUL with more than 4,000 staff delivers 240 world class degree programmes including research across a wide range of subjects in Science and Engineering, Medicine and Dentistry and Humanities. With more than 30,000 students, QMUL is ranked 9th in the UK according to the 2014 Research Assessment Exercise (RAE). Queen Mary is one of 24 leading UK universities represented by the Russell Group, that are committed to maintaining the very best research, an outstanding teaching and learning experience, excellent graduate employability and unrivalled links with business and the public sector.

Queen Mary is also proud to have achieved the national recognition for offering outstanding environment for students that enables stimulating, supportive and high-quality learning experience, with teaching inspired by our world-leading research. Queen Mary ranks top in London among Russell Group universities for student satisfaction (according to the National Student Survey 2016), with a number of our subject areas receiving over 90 per cent for 'overall satisfaction' including Science & Engineering, Medicine, Dentistry, Law and English. Recently, QM

have invested £98m in new facilities and infrastructures over the past five years to offer our students an exceptional learning environment.

QMUL has strong links to the industry and a substantial track record on supporting entrepreneurship. Over the years QMUL has asserted its commitment to cutting-edge R&D producing 6 Nobel Prize winners and incubated several successful hi-tech companies including Activiomics Ltd, Actual Experience Ltd and Retroscreen Virology Group plc. QMUL owns the QTech Software Accelerator, a government funded seed for software inventions. The QTech Software Accelerator is fundamentally about commercialising software innovations originating from research. The aim is to identify commercial opportunities for the software and coach startups in a structured program of education, training and support; boot camps facilitated by externals with commercial expertise; and one-to-one mentoring to develop the pitch. QMUL also owns QApps, a smart phone App Store which distributes a range of innovative and exciting Apps developed by staff and students. QApps is as a collaborative venture supported by Queen Mary Innovation. QMUL hosts one of the UK leading research groups in multimedia signal processing and computer vision – the Multimedia and Vision (MMV) research group.

The Multimedia and Vision Research Group

The MMV group enjoys a distinguished reputation for innovation, receiving direct funding from overseas organisations such as United Technologies, Samsung and the EU. The group has participated and coordinated several EU funded projects relevant to Leader including RACE MAVT; ACTS MOMUSYS, PANORAMA and Custom TV; Esprit, SCHEMA, BUSMAN, NoE K-Space and the COST292 Action. It was one of the main contributors and steering member of FP6 IST Integrated Projects aceMedia and MESH, Co-ordinator of the STReP EASAIER and a partner in RUSHES. In FP7 ICT, the group was core a partner in the STREPs Papyrus and APIDIS, the NoE PetaMedia, REVEIRE (technical coordinator), 3DLife (coordinator), SARACEN, NextMedia and MISSA. In the security domain, MMV was a key participant in the FP7 SEC NoE VideoSense, FP7 ADVISE and FP7 LASIE. The technical expertise gained through the participation of security related projects, will be leveraged in PERSONA. The group also leads several UK EPSRC projects including three industrial CASE projects and the industrial project AUDACE with Visiowave and GE industries. During the past 3 years only, the group has published over 150 journal papers, most of them in the IEE and IEEE Transactions in the field, over 300 refereed conference papers and secured over £7 Million grants funding from various sources.

Key Personnel involved in PERSONA

Prof Ebroul Izquierdo (male) holds the Chair of Multimedia and Vision and is head of the MMV research group. He is a Chartered Engineer, a Fellow member of The Institution of Engineering and Technology (IET), chairman of the Visual Information Engineering professional network of the IET, a senior member of the IEEE, and a member of the British Machine Vision Association. He is also a IEEE distinguished lecturer. He is an associate editor of the IEEE Transactions on Circuits and Systems for Video Technology and has been guest editor of numerous journals. Prof Izquierdo coordinated many European projects namely K-Space, 3DLife and was the technical coordinator for REVERIE. He is also a member of the steering committee of the Networked Electronic Media platform NEM and few other relevant task forces and working groups in NEM and Future Internet Architectures. Prof Izquierdo has published over 500 technical papers and book chapters.



Dr Tomas Piatrik (male) is a senior postdoctoral researcher in the Multimedia and Vision (MMV) Research Group at Queen Mary University of London. His research interests include multimedia analysis, retrieval, machine learning, biologically inspired computing, and video analysis for security and video surveillance domain. He has published over 30 technical papers and reports in various international conferences and book chapters. He has actively participated in several EU funded research projects including K-Space, MESH, PetaMedia, 3DLife, Cubrik and support actions SALA+, NextMedia, Eternals and Conecta2020. His recent research activities in MMV have been focused on video analytics in surveillance as part of the work for EU FP7 Security projects VideoSense, Advise, LASIE and H2020 project SafeShore. Furthermore, he is an organiser of the annual grand challenges on Visual Privacy and in Surveillance and DroneProtect under the MediaEval benchmarking initiative since 2012.



Dr Qianni Zhang (female) received the M.Sc. degree in Internet signal processing in 2004 and the PhD degree in 2007, both from Queen Mary University of London. She is now a lecturer at the School of Electronic Engineering and Computer Science, Queen Mary University of London. Her research interests include multimedia processing and medical imaging. She has published over 30 technical papers and book chapters. She has actively contributed to several past European projects including aceMedia, Busman, K-Space, RUSHES, COST292, 3DLife, Reverie and Ecopix funded by FP7 programme.



Dr. Fiona Rivera (female) PhD, MSc, BSc, BSc, is a postdoctoral researcher at Queen Mary University of London. Dr. Rivera has extensive technical and research experience, specialising in the field of multimedia processing, and has co-authored a technical book and published related research papers. Over the past 6 years, she has enjoyed international reputation as a technology consultant and project manager, contributing towards several EU funded projects including CONNECTA 2020 (H2020), and FP7 projects REVERIE, EMC2 and 3DLife. Dr. Rivera holds a B.Sc. in Economics from the London School of Economics, a B.Sc. from the Open University, an M.Sc. in Multimedia and Virtual Environments from the University of Sussex, and a PhD from QMUL.



Role in the project

QMUL is a leading European research centre with extensive expertise in video analytics for the security domain. QMUL will thus make critical contributions to towards the development of techniques and modules related with video analytics and PERSONA system through leading Study and analysis of latest and new generation no-gate crossing point solutions (T2.1), Video analytics and data fusion for person, object and abnormal behaviour detection (T2.3). As an experienced H2020, and FP7 project coordinator and partner, QMUL are ideally placed to also lead Dissemination, exploitation and liaison with projects lead (WP6), including leading Dissemination planning (T6.1), Dissemination implementation (T6.2), and Liaison with BES-15 and other relevant projects (T6.3). Further contributions will be made to (T1.3) Technical requirements of no-gate crossing point solutions, (T1.4) Definition of PERSONA requirements, (T2.2): Verification scanners and smart sensors, (T2.4): Security assessment and decision support systems, (T2.6): (Technical validation and testing, (T3.3) Questionnaires and metrics development, (T3.4) Orchestration plan and framework specification, (T3.5) Development of orchestration framework for no-gate

technologies assessment, (WP4): Field deployment of no-gate technologies and acceptance assessment, (T4.2) Field deployment of no-gate technologies, (T4.3) Research data collection and management, (T5.1) Creation of Advisory Board, (T5.4) PERSONA textbook of acceptance of no-gate border security solutions, (T6.4) Workshops organisation.

Output and Background Relevant to the targeted R&D in PERSONA

- Large scale knowledge repository and ontology framework for video surveillance domain
- Robust foreground and background subtraction from CCTV footage
- Robust Logo and Distinctive region of interest detection aiding Super Recognisers
- Multi-camera person and object tracking
- Privacy protection and filtering techniques for anonymization of CCTV content
- Intuitive interface design for effective random browsing interface
- An ill-posed operator for secure image authentication
- Data-driven nonlinear diffusion for object segmentation

Publications


- Sobhani, F., K. Chandramouli, Q. Zhang, and E. Izquierdo. Formal representation of events in a surveillance domain ontology. in Image Processing (ICIP), 2016 IEEE International Conference on Image Processing 2016. IEEE.
- Salehe Erfanian Ebadi, Ebroul Izquierdo "Dynamic Tree Structured Sparse RPCA via Column Subset Selection for Background Modeling and Foreground Detection", 2016 International Conference on Image Processing, p.5.
- Salehe Erfanian Ebadi, Ebroul Izquierdo "Foreground Segmentation via Dynamic Tree-Structured Sparse RPCA", 2016 European Conference on Computer Vision 2016, p.16.
- Erfanian Ebadi S., Guerra Ones V., and Izquierdo E., "Efficient Background Subtraction with Low-rank and Sparse Matrix Decomposition", In Image Processing (ICIP), 2015 IEEE International Conference on., September, 2015
- Craig Henderson, Ebroul Izquierdo, Robust feature matching in long-running poor quality videos, IEEE Trans. Circuits and Systems in Video Technology, 2015
- Erfanian Ebadi S., Izquierdo E. (2015), "Approximated RPCA for Fast and Efficient Recovery of Corrupted and Linearly Correlated Images and Video Frames", Systems, Signals and Image Processing (IWSSIP), 2015 International Conference on., September, 2015.
- Craig Henderson, Ebroul Izquierdo, Large-scale forensic analysis of security images and videos, BMVC'2014
- Faranak Sobhani, Nur Farhan Kahar, Qianni Zhang, An Ontology Framework for Automated Visual Surveillance System, Int. Conf. on Content-Based Multimedia Indexing (CBMI), Prague, 10-12 June, 2015
- C. Pantoja, A. Ciapetti, C. Massari, M. Tarentelli, Action Recognition in Surveillance Videos using Semantic Web Rules, ICDP'2015
- Craig Henderson, Ebroul Izquierdo (QMUL), Minimal Hough Forest training for pattern detection in Query by Example video search, BMVC 2015

Relevant Previous projects or activities connected to the subject of this proposal

- EU H2020 collaborative project **SafeShore** (2016-2018), "System for detection of Threat Agents in Maritime Border Environment".

- EU FP7 collaborative project **LASIE** (2014-2017), “Large scale information exploitation of forensic data”.
- EU FP7 small or medium-scale focused project **Advise** funded (2012-2015) “Advanced video surveillance archives search engine for security applications”.
- EU FP7 NoE **VideoSense** (2011-2015) “Virtual centre of excellence for ethically-guided and privacy-respecting video analytics in security”.

4.1.7 Swedish Police Authority, National Forensic Centre (SPA)

Partner Number	Partner Full Name	Member State	Partner Type	
7	Swedish Police Authority	SE	LEA	

Partner Description

The Swedish Police Authority (Swedish: Polismyndigheten) is the central administrative authority for the police in Sweden, responsible for border control, law enforcement, general social order and public safety within the country. The agency is headed by the National Police Commissioner, who is appointed by the Government and has the sole responsibility for all activities of the police. Although formally organised under the Ministry of Justice, the Swedish police is—similar to other authorities in Sweden—essentially autonomous, in accordance with the constitution. The agency is governed by general policy instruments and is subject to a number of sanctions and oversight functions, to ensure that the exercise of public authority is in compliance with regulations. The agency is organized into seven police regions and eight national departments. It is one of the largest government agencies in Sweden, with more than 28,500 employees, of which police officers accounted for approximately 75 percent of the personnel in 2014

Key Personnel involved in PERSONA

Britt-Louise Linnea Wahlberg (Female), is a National expert and technical advisor about Border Control and system management, and process manager and administrator in the IT-process management team under the Border Control. In 2016, she participated in unannounced Schengen evaluation for Narva, EE. (First and second line, checks and procedures included IT). She was also part of the Swedish delegation during Schengen evaluation of Sweden for external borders (air). Britt-Louise is an expert for unannounced Schengen evaluation, Barcelona Airport, ES, and for the Schengen evaluation on SIS/SIRENE in NL.



Dr. Lena Klasén (Female), is appointed as Director of the Swedish Police Authority management team. She has a PhD in Image Coding at University of Linköping, Sweden and has led industrial- and research organizations in Swedish authorities such as Swedish Defence research Agency - FOI, Swedish Defence Material Administration - FMV, Swedish National Laboratory of Forensic Science - SKL and recently the Implementing Committee of the New Police organization - SoU at the Swedish Ministry of Justice. Lena has held several commissions of trust, e-gas board member and expert including being appointed as forensic expert by the US Department of Justice. Her industrial experience includes product portfolio management at Saab and being involved in starting up innovative companies.



Dr. Elisabet Leitet (Female) is a forensic expert at Swedish Forensic National Centre, under the Border Control department. Her areas of expertise include Image analysis, image comparison, facial image comparison, facial automatic recognition, evaluation, Likelihood Ratio and sensor forensics. She received from doctoral degree from Uppsala University in the year 2011. She worked as a researcher at Stockholm University investigating the effect of LyAlpha imaging of spiral galaxies.




Role in the project

SPA is the central administrative authority for the police in Sweden, responsible for border control, law enforcement, general social order and public safety within the country. As an LEA SPA will be a key contributor through leading Use-cases and user requirements (T1.2), and Field deployment planning and preparation (T4.1). SPA will further contribute through participation in: Identification of risks and mitigation controls (T1.6), Research methodology for acceptance assessment (T3.1), Field deployment of no-gate technologies (T4.2), Creation of Advisory Board (T5.1), Creation of network of stakeholders and decision makers (T5.2), Contingency plan and treatment measures (T5.3), Communication of guidelines and best practices to stakeholders (T5.5), and Exploitation roadmap and knowledge transfer (T6.5).

Output and Background Relevant to the targeted R&D in PERSONA

- Border control system
- Document and ID verification
- Image analysis and image comparison
- Facial image comparison
- Facial automatic recognition
- National Facilitation Programs

4.1.8 Bundesrechenzentrum – Federal Computing Centre

Partner Number	Partner Full Name	Member State	Partner Type	
8	Bundesrechenzentrum – Federal Computing Centre	AT	LEA	

Partner Description

The Federal Computing Centre of Austria – Bundesrechenzentrum (BRZ) is the market-leading e-government partner of the federal administration in Austria.

BRZ is in charge of approximately 1,200 employees, 3,000 servers and has equipped 1,200 locations throughout Austria with infrastructure; this service has successfully deployed more than 300 IT-processes. Overall, the BRZ supports more than 400 e-government applications that are used by five million users.

The BRZ runs one of Austria's largest computing centres, its own parallel computing centre and ensures one of the most reliable infrastructures available. The Federal Computing Centre of Austria is also an internationally renowned cooperation partner.

The BRZ develops and operates the main federal eGovernment applications, including the applications of the Federal Ministries of Finance and Justice. Business relevance exhibits a range of applications, over all the Business Service Portal (USP.gv.at) and a range of public registers with business relevance, such as the Gewerberegister, the Company register and the Grundbuch. The BRZ developed and operates the Austrian Customs applications and registers.

Furthermore, the BRZ operates the central Austrian Portal Service, with more than 300 integrated public procedures and serves as an accepted Single-Sign-On for more than 80000 users of the public administration. The Portal Austria received the national and European EuroCloud award in 2012. The experience of the BRZ in business related eGovernment is shown in the participation in the European large-scale pilot project PEPPOL and the membership in OpenPEPPOL,

The BRZ is founding member of the European Association of Public IT Service Providers (EURITAS) and shares information and knowledge at a European scale among the partners. BRZ is assigned by the Austrian Customs Authority BMF to operate the Austrian customs applications. BRZ operates a forensic lab, is part of the Austrian govCERT and operates an own CERT for its own ecosystem. BRZ is part of the critical infrastructure environment in Austria.

- 60 certified project managers
- ISO 27001, 27018, 22301, 9001
- SAP-CCoE
- Member of EURITAS - European Association of Public IT Service Providers
- eGovernment Competence Centre for the Austrian Public Administration

Key Personnel involved in PERSONA

Johannes Mariel (male) is the Chief Information Security Officer (CISO) of BRZ, Member in board of directors in BRZ, lecturer at universities and academies, key note speaker on cybersecurity topics. 39years of working experience, 28 years in ICT/Cybersecurity, 13 years as CISO. Engineer in ICT. Certifications in Risk Management.



Carl-Markus Piswanger (male) is an eGovernment architect, lecturer at universities and academies, several involvements in EU projects. 30 years working experience, 16 years in ICT/eGovernment, master’s in history/Political Science, Post Gradual Master in E-Government and in General Management, Certifications in Project Management, Process Management, Marketing Professional, Certified Management Consultant



Alexander Petioky (male) holds a Master of Business Informatics and is certified as Advanced Professional for Software Architecture (CPSA-A), Enterprise Architect (TOGAF 9 Certified Level). He has 17 years of experience in designing, developing and maintaining applications in the business domain of customs and excise, on national and international level (NCTS, ECS, ICS, SEED, EMCS). Currently he has working on a redesign and new implementation of the booking system of national customs duties and taxes and EU own resources; and supports designing the national implementations of UCC.

Peter Falkensteiner (male) holds a Master of Information Security, has a Certified Information Systems Security Professional (CISSP) and an Information Security Manager (ISO 27000) designation; he has 15 years of professional IT experience and 9 years of experience with governmental services; currently working on design of national implementations of UCC, attended EU ITSDG and CBG meetings.

Michael Hauenschild (male) is a Head Architect for e-Government and e-Health as well as a Security Forensic Analyst at the Federal Computing Center of Austria (BRZ) in Vienna. He is primary responsible for the access and identity management, which is a main part of the BRZ Portal Austria Cloud Solution (Euro Cloud Award Winner 2012), the technical architecture of the Austrian Health Record, Forensic Analyst for Major Incidents and Part of the Incident Response Team. Michael is a graduate engineer of surveying and has several years of experience in different IT environments.

Lorenz Zechner (male) is an IT-Engineer with experience in EU projects: IT-Engineer with involvements in multiple national and EU projects, 12 years of working experience, 4 in eGovernment and 4 in national and international research with focus on IT-Security. MSc in “Business Engineering and Computer Science” and BSc in “Media Informatics and Visual Computing” at the Vienna University of Technology.

Manoela Bodiroza (female) works in International affairs has a master’s in social and Economic Sciences, 11 years working experience in ICT/eGovernment; Certified E-Government Expert; From 2008 – 2012 she was working in the WP7 (dissemination, awareness and consensus building) of the PEPPOL Project, one of the 5 LSP Projects of the European Commission. The main focus of her work was the elaboration and implementation of the dissemination and communication plan, implementation of the website as well as event management. Since 2011 she is leading the Joint Advisory Group of Euritas – the European Association of Public IT Service Provider and responsible for international topics, esp. EU funded projects.

Role in the project

The Federal Computing Centre of Austria – Bundesrechenzentrum (BRZ) is the market-leading e-government partner of the federal administration in Austria. The BRZ develops and operates the main federal eGovernment applications, including the applications of the Federal Ministries of Finance and Justice. BRZ will provide key contributions towards use-cases and user requirements

(T1.2), Field deployment planning and preparation (T4.1), and Field deployment of no-gate technologies (T4.2).

Output and Background Relevant to the targeted R&D in PERSONA

- Detlef Hühnlein, Carl-Markus Piswanger (et.al.): FutureTrust – Future Trust Services for Trustworthy Global Transactions, in: M. Talamo, H. Roßnagel, D. Hühnlein, C. Schunck (Ed.): Open Identity Summit 2016, Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016, Page 27-41
- Linda Strick, Carl-Markus Piswanger: Cloud Computing in the Public Sector – Key Factors and Lessons Learned from the EU-Project «Cloud for Europe» (IRIS 2016, Proceeding), Page 637-644
- Carl-Markus Piswanger; Linda Strick: European innovation procurement “Pre-Commercial-Procurement” and Cloud computing by reference to the research project “Cloud for Europe” (IEEE, ICEDEG 2017) Page 161-166
- Kieseberg, Peter, Weippl Edgar, Zechner Lorenz: IN-MOTOS: Extending the ROPE-methodology - in: 14th International Conference on Information Integration and Web-based Applications and Services (iiWAS2012)

Relevant Previous projects or activities connected to the subject of this proposal


- **TOOP –The-Once-Only-Principle (H2020)** aims to explore and demonstrate the “once-only” principle (OOP) on a cross-border pan-European scale by developing a generic federated architecture that is able to connect registries and e-government architectures in different countries. TOOP is unique in its ambition and scale, aiming to connect 60 information systems from at least 20 countries. www.toop.eu
- **FutureTrust (H2020)** aims at supporting the practical implementation of the eIDAS regulation in Europe and beyond. For this purpose, the FutureTrust project will address the need for globally interoperable solutions through basic research with respect to the foundations of trust and trustworthiness, actively support the standardisation process in relevant areas, and provide Open Source software components and trustworthy services which will ease the use of eID and electronic signature technology in real world applications. In particular the FutureTrust project will extend the existing European Trust Service Status List (TSL) infrastructure towards a “Global Trust List”, develop a comprehensive Open Source Validation Service as well as a scalable Preservation Service for electronic signatures and seals and will provide components for the eID-based application for qualified certificates across borders, and for the trustworthy creation of remote signatures and seals in a mobile environment. The present contribution provides an overview of the FutureTrust project and invites further stakeholders to actively participate as associated partners and contribute to the development of future trust services for trustworthy global transactions. <https://www.futuretrust.eu/home/>
- **PEPPOL – Pan European Public Procurement Online.** The Pan-European Public Procurement Online (PEPPOL) project was a pilot project funded jointly by the European Commission and the PEPPOL Consortium members. The PEPPOL project was initiated in 2008 with the aim of simplifying electronic procurement across the borders by developing technology standards that could be implemented across all governments within Europe. The overall objective was to enable businesses to communicate electronically with any European government institution in the procurement process, increasing efficiencies and reducing costs <http://www.peppol.eu/>

- **eCodex** – The e-CODEX project improves the cross-border access of citizens and businesses to legal means in Europe and furthermore creates the interoperability between legal authorities within the EU. In pursuing this goal, e-CODEX is developing building blocks that can be used in or between Member States to support cross-border operation of processes in the field of justice. e-CODEX shows that this is possible in various fields. Besides the technical achievements, the e-CODEX partner countries agreed on formal procedures how to integrate judicial procedures for e-Justice - its pilots as well as for future scenarios. <https://www.e-codex.eu/>
- **Cloud4Europe (FP7)** supports public sector cloud use as collaboration between public authorities and industry. The project identifies obstacles, finds innovative solutions and builds trust in European cloud computing. Cloud for Europe uses pre-commercial procurement as an instrument for public sector innovation. The pre-commercial procurement identifies innovative solutions for cloud services that best fit public sector needs, but also provides better information to public procurers about the potential of cloud services. <http://www.cloudforeurope.eu/>
- **SSEDIC** The objective of this network is to provide a platform for all the stakeholders of eID (electronic identity) to work together and collaborate to prepare the agenda for a proposed Single European Digital Identity Community as envisaged by the Digital Agenda (DAE) in its Key Action 16. <http://www.eid-ssedic.eu/>
- Several Twinning projects, and more than 300 national ICT project/year within the Austrian public administration.

Significant infrastructure and/or any major items of technical equipment that's relevant to the proposed work

- BRZ represents a critical infrastructure in Austria
- eFinance applications (Finance Online, Customs, and others)
- Portal Austria (Access Management, Identity Management, Content Management, Security Applications, integrated Austrian eGovernment applications), based on that applications the biggest eGovernment portals are implemented
- Central eHealth applications (ELGA)
- eJustice applications
- eGovernment eID Services, Signature Services, Trust Services
- Governmental ICT infrastructure and security infrastructure
- BRZ Security Infrastructure following high requirements from ISO27001/ISO27018 (Information Security Management)
- Federal Predictive Analytics Applications and Infrastructure
- Federal Big Data Shared Service Application and Infrastructure

4.1.9 Ministry of Interior of the Republic of Serbia (SMOI)

Partner Number	Partner Full Name	Member State	Partner Type	
9	Ministry of Interior Republic of Serbia	RS	LEA	


<p>Partner Description</p>
<p>Ministry of Interior of the Republic of Serbia performs state administration tasks relating to the protection of life, property and personal security of citizens; prevention and detection of crime and finding and catching offenders and bringing them to the relevant authorities; maintenance of public order; providing assistance in case of emergency; securing public gatherings and other public meetings; the providing security of certain persons and objects, including foreign diplomatic and consular missions of the Republic of Serbia; safety, regulation and control of traffic on the roads; state border security and border and movement and residence within the border zone; Stay of Foreigners; Traffic and transportation of firearms, ammunition, explosives and certain other hazardous substances; testing of small arms, ammunition and devices; fire protection; anti-hail; citizenship; unique identification number; electronic management of personal data; domicile and residence; ID card; passport; international aid and other forms of international cooperation in the field of internal affairs, including readmission; illegal migration; asylum; training of personnel; administrative resolution on appeal pursuant to regulations on refugees, as well as other duties specified by law.</p> <p>The state administration affairs defined by Serbian legislation and regulations adopted pursuant to the legislation are performed by the ministries. They apply laws and other regulations and general acts adopted by the National Assembly and Government, as well as the general acts rendered by the President of the Republic; they address administrative issues, conduct administrative supervision of the performance of assigned tasks, etc.</p> <p>The Ministry of Interior (MOI) is fully committed to improvement of the overall efficiency and effectiveness of its main functions in order to deliver a better service to the citizens of Serbia.</p>
<p>Key Personnel involved in PERSONA</p>
<p>Zoran Vasković (Male), is a national expert in area of border management, and coordinator about Border Control and Surveillance on all types of border crossing points. He has more than 30 years of experience in area of border management and passing duties from the operative one to the strategic. Actively involved in gathering overall picture of state on border management in whole territory of Republic of Serbia and conducting processes connected to the development of Integrated border management Strategy with following Action Plan. In charge for the Coordination in processes related to harmonisation of national legislation with EU acquire in domain of competence of Border Police.</p> <p>Vladimir Lekic (Male), is software developer with more than 5 years of experience in development software solution for person, documents and vehicle control on border crossing point. Solution which is in use is completely developed in house, and supported adjustment according Border police request in line with national legislation. He has great experience in integrated solution development integrating connection with other relevant system on national level as external systems as it is checks via web services according Interpol databases.</p> <p>Snežana Stojičić (Female) is responsible for the coordination and project management and international affairs, especially in scope of EU integration and technical requirements for harmonization Republic of Serbia with EU acquire. She has over 30 years' experience in ICT sector, in design and implementation IT projects. Taking part in analysing and following national and international standards and regulation from aspect of needed technical requirements for implementation and in developing strategic documents.</p>
<p>Role in the project</p>

As an LEA SMOI will be a key contributor through participation in Use-cases and user requirements (T1.2), and Field deployment planning and preparation (T4.1). SMOI will further contribute through participation in: Identification of risks and mitigation controls (T1.6), Research methodology for acceptance assessment (T3.1), Field deployment of no-gate technologies (T4.2), Creation of Advisory Board (T5.1), Creation of network of stakeholders and decision makers (T5.2), Contingency plan and treatment measures (T5.3), Communication of guidelines and best practices to stakeholders (T5.5), and Exploitation roadmap and knowledge transfer (T6.5).

Output and Background Relevant to the targeted R&D in PERSONA

- Mol's Intranet Network and Extranet network segment
- Border management
- Border control system
- Existing eGate solution
- Document and ID verification
- Software development
- Risk assessment in the border management

4.1.10 Ministry of Public Security – Israel National Police (MOPS)

Partner Number	Partner Full Name	Member State	Partner Type	
10	Ministry of Public Security – Israel National Police	Israel	LEA	

Partner Description

The Israel National Police (INP) is under the Ministry of Public Security (MOPS), comprised of some 30,000 sworn officers reinforced by 50,000 volunteers. It is the sole responsible of policing and law enforcement in Israel. The responsibilities of INP cover all aspects from the local through the national levels.

The Israel National Police is guided by the values and principles of the democratic government of the State of Israel. The main areas on which the Israel Police focuses are:

Public Security - The prevention and thwarting of terror, response to calls from citizens, arrangement of security procedures and organization of volunteers (Civil Guard).

Maintaining Law and Order - Response to calls regarding public disturbances, effective response to demonstrations and unlawful gatherings, licensing – establishment of limits and conditions for businesses, responsibility for detainees and implementation of court orders.

Fighting Crime - Investigation of crimes and apprehension of offenders, detection and exposure of unreported crimes such as drug trafficking, extortion and instructing to the public how to protect themselves and their property.

Traffic Enforcement - Directing traffic and working to ensure smooth traffic flow, enforcement of traffic laws, investigating traffic accidents and apprehension of traffic offenders. In addition, instructing the public on traffic safety and participation in the decision-making process in such matters as the planning and construction of roads, placement of road signs and traffic lights.

Border Security – The Border Police Serves as the operational arm of the Israel National Police. The multi-purpose force deals with challenges relating to public security, terror, severe crime, rioting, guarding sensitive sites and securing rural areas.

Division of Identification and Forensic Science (DIFS)

Israel National Police Division of Identification and Forensic Science (DIFS) is part of the investigations and Intelligence branch and is situated in the Israeli police National Headquarter in Jerusalem.

Dedicated Laboratories and units, specializing in the wide variety of scientific and technological fields, provide services to diverse police units in the national effort for fighting crime. Those services include scientific analysis and evidence, technical support, training and experts witness testimony in our courts of law.

Their functions within the division include Safety and Quality Assurance, logistics and on-going research and development. The Division has the globally recognized ISO 17025 accreditation.

Investigation and Intelligence Department - Technological Unit

The unit is part of the investigations and Intelligence branch of the Israel National Police (INP) and responsible of carrying out, leading and participating in projects related to technological aspects in the department.

Major mission of the unit is to find and keep up to date new technologies, software and systems for the use of the INP investigators and intelligence officers.

Research and Development Division (R&D division)

The R&D Division in the Israel National Police (INP) introduces new and updated technological means for improving the operational ability of the INP to fulfil its duties according to the law.

The activity of the R&D Division varies from pure research and development to implementation of changes to existing means.

The R&D Division is part of the Technologies Administration (TA) lead by a Brigadier General and besides its main purpose, as described above, it is also coordinates the technological cooperation of the INP on behalf of the Deputy Commissioner.

Key Personnel involved in PERSONA

Superintendent Dr. Netta Lev Tov Chattah (female) is the Head of the Laboratory of Digital Evidence at the Israel National Police (INP), Department of Identification and Forensic science. The lab focuses on forensic facial examination and identification cases from digital media and is responsible for managing the mug shot repository. She is a facial examination expert and an active participant in the **Facial Identification Scientific Working Group** as well as the Facial Identification Subcommittee of the **Organization of Scientific Area Committees of the US Government**. She is also involved in the **Interpol**



Facial Expert Working Group and partakes in activities contributing to research on the human ability to match unfamiliar faces from photos in different scenarios. Superintendent Netta has a PhD. in Bio anthropology and has done postdoctoral research on calcified tissue biomechanics. Her academic work has been published in scientific journals.

Superintendent Maja Engelhard (female) is the Head of the Profiling & Research field in the Investigative Psychology Unit in the Division of Identification & Forensic Sciences at the Israel National Police (INP) Headquarter, and serving over 15 years in this position. She has 20 years of investigative psychology experience. The Investigative Psychology covers Polygraph tests, Profiling, Cognitive Interviews and other requested psychological manipulations during criminal investigations. Mrs. Engelhard, in her current position, is responsible for the development and implementation of applied and innovative applications in the field of offender profiling. She is the founder of the profiling field in INP and considered to be a specialist and a center of knowledge in the field of applied offender profiling, giving lectures and workshops in INP and other Law Enforcement Agencies around the world. In her previous position, Mrs. Engelhard was the head of a research team who developed an applied model of offender profiling for rape, murder, indecent assault and aggravated robbery. During the years Mrs. Engelhard participated and influenced in a wide range of criminal and terrorists' investigations. Mrs. Engelhard has a Bachelor of Science degree (BSc) in Psychology from Nottingham University and has a Master of Science degree (MSc.) in Investigative Psychology from Liverpool University.

Mr. Saar Semo (male) is a Technology consultant for investigations and intelligence Division at the Israel National Police over three years. Major part of his responsibilities is to find new "breaking point" technologies and systems.

Mr. Semo has acquired an extensive experience as part of the consulting – Project management technology in a national project between Israeli law enforcement agencies and the Financial sector in Israel. Mr. Semo is a member at Visual intelligence technological project at Israel National Police. Mr. Semo has 10 years of experience in system management technologies, including SIEM/SOC technologies in financial institution.

Commander Ofer Shenhav (male) is the Head of the R&D Division at the Israel National Police (INP) Headquarter, and serving in the INP for over 17 years. Mr. Shenhav, in his current position, is responsible for the development of innovative technology in the fields of Electronics, Mechanics and Chemistry related to public safety and Home land security (HLS). In his previous position he managed the Software Engineering department of the INP specializing in the fields of Information Technology (IT) and GIS data systems. Mr. Shenhav also worked and an IT developer in the group of Information Systems & Technologies in the Ministry of Defence for 7 years. Between the years of 1977- 1986 He was a Technology Officer at the Israel Defence Forces (IDF) Mr. Shenhav has bachelor's degree (B.S.C) in Computers science and Mathematics from Tel Aviv University and has master's degree in business administration (M.B.A) of Management Information Systems From New York Institute of Technology.



Mr. Chad Leibner, M.Sc. (male) has been serving in the Israel National Police (INP) for over 20 years, and has extensive experience in many aspects of police work and managing R&D projects. As the Chemistry & Materials officer in the R&D division, Superintendent Leibner is has extensive knowledge in certain fields of substances and substances identification technologies.

As LEAR to HORIZON 2020 for the Ministry of Public Security & Israel National Police, Mr. Leibner has extensive knowledge in legal and financial aspects regarding the EU framework programs. Mr. Leibner is the representative of the INP for the ILEAnet project (HORIZON 2020) and has



participated in the following FP-7 projects: SNIFFER; AEROCEPTOR; SUBCOP Mr. Leibner has a MSc. in chemistry from the Hebrew University in Jerusalem.

Role in the Project: LEAR for MOPS (INP)

Role in the project

As an LEA MOPS will add their extensive experience to contribute towards PERSONA outcomes through participation in Field deployment planning and preparation (T4.1), and Field deployment of no-gate technologies (T4.2). MOPS will also be a valuable contributor towards Use-cases and user requirements (T1.2), methodology for acceptance assessment (T3.1), Creation of Advisory Board (T5.1), Creation of network of stakeholders and decision makers (T5.2), Contingency plan and treatment measures (T5.3), Communication of guidelines and best practices to stakeholders (T5.5), and Exploitation roadmap and knowledge transfer (T6.5).

Output and Background Relevant to the targeted R&D in PERSONA

- Facial recognition
- Behaviour and micro-expression analysis
- law enforcement and combatting crime
- maintaining public order and protecting the public from terror attacks;
- preventing violence and delinquency in society;

Relevant Previous projects or activities connected to the subject of this proposal

Horizon 2020:

- **LAW-TRAIN:** Mixed-reality environment for training teams in joint investigative Interrogation-Intelligent interrogation training simulator
- **SafeShore:** System for detection of Threat Agents in Maritime Border Environment. (www.safeshore.eu)

FP-7:

- **AEROCEPTOR:** UAV Based Innovative Means For Land And Sea Non-Cooperative Vehicles Stop.
- **CAPER:** Collaborative information, Acquisition, Processing, Exploitation and Reporting for the prevention of organized crime.
- **MEPROCS:** New methodologies and protocols of forensic identification by craniofacial superimposition.
- **SUBCOP:** Suicide Bomber Counteraction and Prevention.

4.2 Third Parties Involved in the Project (including Use of Third Party Resources)

Please complete, for each participant, the following table (or simply state "No third parties involved", if applicable):

Does the participant plan to subcontract certain tasks (please note that core tasks of the project should not be sub-contracted)	No
If yes, please describe and justify the tasks to be subcontracted	



Does the participant envisage that part of its work is performed by linked third parties	No
If yes, please describe the third party, the link of the participant to the third party, and describe and justify the foreseen tasks to be performed by the third party	
Does the participant envisage the use of contributions in kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)	No
If yes, please describe the third party and their contributions	

5 Ethics and Security

5.1 Ethics

The storage and analysis of large amounts of forensic data as envisaged by the PERSONA project engages legal and ethical issues. The primary concern is the possession and manipulation of person data. Such possession and manipulation are regulated by the several legal regulations and ethical norms.

5.1.1 Privacy and data protection

Though privacy is a fundamental right, it is not absolute. Important for our purposes are the requirements imposed both by the European Convention of Human rights to assess legitimate interference with the right to privacy (the 'limitation test'). Following the wording of Art 8(2), any interference with privacy must be: (1) prescribed by law (i.e. legality), (2) necessary in democratic society (i.e. necessity), and (3) serve the certain public interest (i.e. legitimacy). In other words, any interference must have a firm, clear, explicit and foreseeable legal basis and must be proportionate to the legitimate aim pursued, i.e. must 'correspond to a pressing social need.' Some methods to assess lack of proportionality include manifest disproportionality or existence of an alternative and less intrusive solution.

Privacy is a constitutional standard in contemporary European democracies. It is considered as a 'first' generation fundamental right, i.e. a political freedom. Both the European Convention of Human Rights and Charter of Fundamental Rights are of uniform application throughout their territorial scope, yet the states enjoy certain margin of appreciation. The European Court of Human and European Court of Jus-tice observe uniform application of the Convention and of the Charter. Thus, the concept of privacy could be regarded as being of uniform nature within each of these systems.

National laws are supposed to conform to this uniform standard, especially in case of a lack of EU-wide regulatory scheme for smart grids (metering) or before such a scheme enters into force. Moreover, the EU's respect for fundamental rights and an explicit reference to ECHR in Art 6 of the Treaty of European Union obliges also the Union to observe this standard.

5.1.2 General data protection principles

According to general rules of data protection, personal data must be: fairly and lawfully processed [Art 6(1)(a)], collected for specific, explicitly defined and legitimate purposes [Art 6(1)(b)] and not further processed in a way incompatible with those purposes [Art 6(1)(b)] (data minimisation) and retained only for as long as is necessary to fulfil that purpose – Art 6(1)(c) (implicitly). The principle of 'data quality' assures that data is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed [Art 6(1)], accurate and, where necessary, kept up to date [Art 6(1)(d)]

Furthermore, there must be a legitimate basis for processing data (Art 7), and unambiguous consent of the data subject [Art 2(h)], meaning, in other words that there must be a contract to which the data subject is a party, that compliance with a legal obligation of the data controller, that protection of the vital interest of the data subject, that performance of the task carried out in the public interest or exercise of official authority and that legitimate interest is pursued by the controller. Data must be anonymised [Art 6(1)(e)] and kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Data collected must be secure, meaning that its process will be done in a confidential (Art 16) and security (Art 17) i.e. with appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss,



alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Finally, subjects shall be completely notified about data processing, that is, controller must notify the national supervisory authority before carrying out any wholly or partly automatic processing operation [Art 18(1)], subject to certain exceptions, e.g. appointing the in-house data protection official [Art 18(2)].

Processing of certain categories of data is prohibited, i.e. revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life [Art 8(1)]. The Data Protection Directive introduces a stricter and prohibitive regime for sensitive data.

Member States may, for reasons of substantial public interest, lay down exemptions in addition to the above mentioned [Art 8(4)]. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority [Art 8(5)]. The Commission must be notified about such derogations [Art 8(7)]. Processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression is allowed [Art 9].

Transfer of personal data to jurisdictions without adequate level of protection is prohibited (Art 25), unless it is covered by one of the following exceptions [Art 26(1)]: explicit unambiguous consent of the data subject, contract or pre-contractual measures, contract between controller and a third party in the interest of the data subject, important public interest, vital interest of the data subject, transfer from a public register, authorisation by Member State [Art 26(2)]. The European Commission determines what jurisdictions provide the adequate level of protection [Art 25(6)].

5.1.3 Relevant legal regulations

At the international level, the right to privacy is protected by Art 12 of the Universal Declaration of Human Rights (1948), which is however non-binding, and Art 17 of the International Covenant on Civil and Political Rights (1966). In 1980, the OECD issued the Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data.

Protection of privacy and personal data at the European (regional) level is based on two systems. The first one, i.e. the Council of Europe (CoE), is based on the Art 8 of the European Convention on Human Rights (ECHR) and sector-specific instruments, namely the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108) with an additional protocol regarding supervisory authorities and trans-border data flows (No 181). In addition, the Council of Europe's Committee of Ministers adopted a number of recommendations to its member states concerning data protection. The ECHR establishes the European Court of Human Rights (ECtHR) in Strasbourg. While the ECHR itself is silent about protection of personal data, the Court has developed it from the right to privacy.

The other arrangement (i.e. the European Union) is based on the EU Treaties, the Charter of the Fundamental Rights (CFR) and secondary legislation, namely the Directives. After the entry into force of the Lisbon Treaty (2009), the CFR became a legally binding instrument and the Treaties now include explicit reference to protection of personal data. Art 16 (formerly Art 286) of Treaty on the Functioning of the European Union (TFEU) and Art 39 of Treaty of the European Union (TEU) both recognise the right to data protection. Art 7 of the CFR provides the right to respect for private and family life and its Art 8 provides for the protection of personal data. The Court of Justice of the European Union in Luxembourg (colloquially the European Court of Justice, ECJ) ensures uniform application of the EU law. The EU secondary legislation consist of three 'basic' instruments: the Data



Protection Directive (95/46/EC),³⁰ the ePrivacy Directive (2002/58/EC),³¹ as amended by Directives: 2006/24/EC and 2009/136/EC,³² and the Data Retention Directive (2006/24/EC).³³ The ‘specific’ instruments consist of: Council Framework Decision 2008/977/JHA³⁴ (dealing with data protection with regard to criminal matters, i.e. former 3rd pillar), and Regulation 45/2001³⁵ (laying down data protection rules for the EU institutions and bodies).

5.1.4 The European Union’s data protection framework

The 1995 Data Protection Directive constitutes a three-level system. The first level is the general one that applies to any processing of personal data. The second level, which needs to be applied on top of the first level, is applicable when sensitive data are being processed. The third level is applicable when personal data are being processed to third countries, i.e. outside the European Union/European Economic Area. A directive is an EU legal instrument that is not directly applicable in the Member States. Thus, each of them needed to implement it in their legal systems. Therefore, we have at least 27 national laws governing data protection in the EU.³⁶ The Directive does not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law (i.e. former 2nd and 3rd pillar of the EU) and by a natural person in the course of a purely personal or household activity [cf. Art 3(2)].

5.1.5 Protection of privacy and personal data in police and judicial cooperation in Europe

There is a different set of rules in the EU applicable for processing personal data for the purposes of police and judicial cooperation. The extensive deployment of surveillance technologies in criminal proceedings has shifted the focus from post-crime to pre-crime situations. As a consequence, policing and criminology have gained a central stage in criminal proceedings, overshadowing the corrective and rehabilitative function of punishment in criminal law. As De Hert and van Brakel note,

³⁰ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

³¹ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

³² Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

³³ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

³⁴ Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

³⁵ Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

³⁶ Cf. the national implementations of the Data Protection Directive at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:71995L0046:EN:NOT> or at http://ec.europa.eu/justice/policies/privacy/law/implementation_en.htm.

a shift to a more proactive, predictive and pre-crime society is one of the main trends emerging in policing, criminology and surveillance studies.³⁷

The first question is whether Art 6 applies to pre-trial investigation. It guarantees procedural rights of parties to civil proceedings and rights of the defendant (accused suspect) in criminal proceedings. Whereas other participants in the trial (victims, witnesses, etc.) have no standing to complain under Article 6, their rights are often taken into account by the European Court of Human Rights.³⁸

Secondly, once the evidence is based on material obtained from video surveillance, a number of classical criminal law procedural guarantees can have the same effects as data protection principles.³⁹

The principle of the due process of law (fair trial) is wide in its juridical nature and includes a set of rights which can be summarised as follows: the right to be presumed innocent; the right to be informed of the accusation; the right to adequate time and facilities; the right to defend oneself and to have the assistance of a counsel; the right to test witness evidence; the right to free assistance of an interpreter; the right to appeal; the right to compensation for wrongful conviction; the protection against double jeopardy and the privilege against self-incrimination.⁴⁰

The main effects of surveillance on the due process of law concern the right to equality before the law, as surveillance can discriminate individuals against other individuals, and the right not to incriminate oneself, which protects the accused against torture and against false statements or criminal charges,⁴¹ the right to defence, as the processing of an individual's criminal profile before conviction risks making it harder for the accused to prove his/her innocence, and the presumption of innocence.

5.1.6 The revision of the EU data protection framework

On 25 January 2012 the European Commission proposed a new legal framework for data protection in the EU. It consists of two main proposals: one for the General Data Protection Regulation,⁴² meant to replace the 1995 Data Protection Directive, and the Police and Criminal Justice Data Protection Directive,⁴³ meant to replace the Framework Decision 2008/977/JHA. The proposed reform is a fruit of some two years of preparations and it opens up a law-making process that is intended to take at

³⁷ van Brakel, Rosamunde and Paul De Hert, 'Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology-based strategies', *Journal of Police Studies*, 2011, Issue 20, Vol. 20, No. 3, pp. 163-192, p. 3.

³⁸ http://www.coe.int/t/dghl/cooperation/capacitybuilding/Source/documentation/hb12_fairtrial_en.pdf

³⁹ Cf. CoE rep 2002, at 24.

⁴⁰ For a detailed analysis on the legal safeguards in criminal proceedings, see Trechsel, Stephen, *Human Rights in Criminal Proceedings*, cfr. supra note 8.

⁴¹ De Hert, Paul 'Balancing Security and Liberty within the European Human Rights Framework. A Critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11', *Utrecht Law Review*, Vol. 1, Issue 1, September 2005, pp. 69-96, p. 86.

⁴² European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25 January 2012, COM (2012) 11 final.

⁴³ European Commission, Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, Brussels, 25 January 2012, COM (2012) 10 final.



least as much time. One of the main aims of the proposal is to provide an adequate response to the contemporary challenges of the information society.

The reform proposes considerable changes. According to the Commission's press release, the key changes in the data protection reform include a single set of rules on data protection, valid across the EU. It will be a regulation and not a directive, thus once adopted and entered into force, it would be directly applicable in all Member States. This is an important and far-reaching development; once finalized, the new instrument is expected to affect the way Europeans work and live together.⁴⁴In the new arrangement, necessary administrative requirements, such as notification requirement, will be removed. Instead, the Regulation provides for increased responsibility and accountability for those processing personal data. These accountability tools would include data breach notification, appointment of the internal data protection officer and an obligation to conduct a data protection impact assessment. According to the proposal, organisations will only have to deal with a single national data protection authority in the EU Member State where they have their main establishment. Likewise, people can refer to the data protection authority in their country, even when their data is processed by a company based outside the EU. Wherever consent is required for data to be processed, it is clarified that it has to be given explicitly, rather than assumed. As a consequence, individuals will have easier access to their own data and be able to transfer personal data from one service provider to another more easily (right to data portability). The so-called 'right to be forgotten' will help people better manage data protection risks online: people will be able to delete their data if there are no legitimate grounds for retaining it. EU rules must apply if personal data is handled abroad by companies that are active in the EU market and offer their services to EU citizens. Independent national data protection authorities will be strengthened so they can better enforce the EU rules at home. They will be empowered to fine companies that violate EU data protection rules. A new Directive will apply general data protection principles and rules for police and judicial cooperation in criminal matters. The rules will apply to both domestic and cross-border transfers of data.

5.1.7 PERSONA Ethical Management Strategies

PERSONA will ensure reception of all required approvals during the course of the project, especially regarding data capturing sessions, trials and demonstrations. Towards receiving these approvals PERSONA will submit (to the boards granting the approvals) all the required documentation, including informed consent form(s), actor role form(s), as well as a thorough description of the project, the pilots and the testing procedures. A copy of this documentation will be also sent to the EC/REA prior to any data collection or tests.

Ethical rules and regulations stemming from national laws and directives (notably in the countries where the tests will be carried out, UK, Belgium, The Netherlands, Sweden, Romania, Italy, Norway and Israel) will be fully respected. Such national directives may require additional targeted ethical interventions. PERSONA will ensure compliance with both EU directives and national directives (at the countries where pilots, trials and tests will be performed).

5.1.7.1 Recruitment procedures for test subjects

In general, two categories of human participants may be involved in data collection:

- *members of the public* (e.g. bystanders coincidentally present in a captured scene) and
- *voluntary participants* (recruited by PERSONA).

⁴⁴ De Hert & Vagelis



All recorded/captured data that is sensitive, will undergo processing to render it anonymous and will be operated upon its entirety. By sensitive, we mean data that might reveal the identity of a person, of any member of the public.

The voluntary participants are:

- either selected persons e.g. informed members of the public who have consented to an assigned “token role” in the sketches and have accepted to be detected and tracked by cameras;
- other selected persons who have been assigned a greater role in the unfolding of a scenario, and “acting” in the data collection exercise according to their role in the scenario (e.g. “technology equipped policeman”, “suspected terrorist”, etc.).

A strict procedure for the selection of the voluntary participants for the PERSONA trials will be defined and approved by the Ethical expert (MoJ) of the project. The main aspects of the recruitment procedures will become even more detailed during the course of the project implementation.

5.1.7.2 Specific measures to protect the privacy of members of the public

- Information about data collection locations and images/videos potentially capturing the identity of bystanders and actors will be stored anonymously in a secure database and will be destroyed as soon as the study/research task is completed and in any case will be automatically destroyed at the end of the project. Access to the database will be permitted only to authorized personnel, whose access is controlled through secure authentication techniques.
- Any accidental or incidental collection of data (including video data) by the PERSONA monitoring system, that might be related to personal information of actors and bystanders which could be used to identify the person, will be blurred before being made public.
- PERSONA will notify bystanders of public and private spaces employed in all data collections and testing of the monitoring system. This will be implemented by posting a notice visible from all access points to the employed area.

5.1.7.3 Specific measures to protect the privacy of voluntary participants

- The voluntary participants who agree to take part in a specific exercise will only do so after being fully informed of the nature of the exercise and after signing a document confirming their informed consent. A template for such a document is provided at the end of section 4.2 (“PERSONA Consent Form”).
- Each potential voluntary participant will be provided with an information sheet describing the LASIE project, an explanation on the particular research activity related to the exercise, the information to be collected and how that information will be used.
- The “PERSONA Consent Form” (a template can be found at the end of section 5.1.10) will inform voluntary participants that raw or edited (for demonstration purposes) photographs or video recordings depicting them may be included in the final report of PERSONA. The use of such photos and videos in the final report of PERSONA is deemed necessary for the following reasons:
 - To properly demonstrate project technologies, equipment and capabilities in an operational and research setting.
 - To considerably strengthen the value of testing and evaluation by helping determine technology readiness for deployment (e.g. a next phase of the project in a future research program).



- All data containing private information will be destroyed upon completion of the respective study/research task. In any case all personal data will be destroyed automatically at the end of the project and only anonymous or non-identifiable data will be retained after the completion of the final report.

5.1.8 Security measures for storage and handling of data

PERSONA will use state-of-the-art technologies for secure storage, delivery and access of personal information, as well as managing the rights of the users. In this way, there is complete guarantee that the accessed, delivered, stored and transmitted content will be managed by the right persons, with well-defined rights, at the right time.

State-of-the-art firewalls, network security, encryption and authentication will be used to protect collected data. Firewalls prevent the connection to open network ports, and exchange of data will be through consortium known ports, protected via IP filtering and password. Where possible (depending on the facilities of each partner) the data will be stored in a locked server, and all identification data will be stored separately.

Intrusion Detection systems will monitor anomalies in network traffic and activate restraint policy if needed. A metadata framework will be used to identify the data types, owners and allowable use. This will be combined with a controlled access mechanism and in the case of wireless data transmission with efficient encoding and encryption mechanisms.

5.1.9 Protection of Ethnic and other sensitive Information of Participants

Various social stereotypes tend to ascribe specific kinds of criminal behaviour to individuals or groups having specific social characteristics (i.e. gender, race, religion, sexual orientation, political beliefs, ethnicity etc). While devising the various PERSONA pilots and field demonstrations to be tested, the following concrete measures will be enforced to safeguard against stigmatization of groups and individuals on account of their gender, race, religion, sexual orientation, political beliefs, ethnicity, and other social characteristics:

- Volunteers acting in the scenarios will assume the various roles (both the roles involving criminal action as well as the roles involving counter criminal action) in such a way that those roles will refer to a variety of different social characteristics in a random manner (i.e. gender, race, religion, sexual orientation, political beliefs, ethnicity etc).
- A variety of crime types will be studied in order to minimize the chance of evoking social stereotypes for specific types of crimes.
- D8.1 “Pilot Definition, Planning and Preparation” will be referred to the Security Assessment Committee prior to its official submission to the EC, for evaluation of the devised scenarios, specifically regarding possible stigmatization of groups and individuals on account of their gender, race, religion, sexual orientation, political beliefs, ethnicity, and other social characteristics.

5.1.10 Informed Consent

Gaining formal consent is an essential element of ethnically valid social research. Each participant, including members of PERSONA consortium, will be informed before each data collection exercise and test session on the ethics directives, principals and implications and they will be invited to sign a consent form. The Consent Form will be tailored specifically to each different test/technology (e.g., audio technologies, video technologies). In all cases volunteers can withdraw at any time during any exercise and test session. The Informed Consent Form to be used in PERSONA is presented in a following paragraph.



Beyond the Exercise Plan Form and Actor Role Form, each potential voluntary participant will be provided with an information sheet describing the PERSONA project, an explanation on the particular research activity related to the exercise, the information to be collected and how that information will be used.

Important note: *No involvement of children or adults unable to give consent is envisaged in the PERSONA project. Such involvement is not deemed necessary for the purposes of the project or the successful realization of the project's use cases.*

PERSONA Informed Consent Form

Purpose of data collection: *The following data will be collected for the EU research project PERSONA funded by European Commission under the Security area of the Seventh Framework Programme (FP7-SECURITY). PERSONA will use this data for research and development, training, validating and evaluating human cognitive, psychological and neuropsychological models.*

PERSONA Consortium Contact Point(s): <Names of the Ethical Expert: **NCP**>

Who has access to this information: By signing the form you give your consent to collect visual, audio or other data related to you with your possible participation in the images and your voice in the acoustic clips. The PERSONA ethical experts will be the only members of the project that will have access to your personal information. The PERSONA Consortium members who see/access this information have already signed a strict confidentiality agreement and will keep the information confidential. PERSONA researchers will have access to anonymous data only. The final report of the PERSONA project may contain raw or edited versions of the collected data for demonstration purposes.

Withdrawal Information: Your participation in the PERSONA project is completely voluntary, and you can choose to stop participating at any time. If you decide to withdraw from the project, please contact the PERSONA consortium contact points outlined above, and they will explain the best way for you to stop taking part.

You should know that you may be withdrawn from the project for any of the following reasons:

- If you do not follow the project's Ethical expert's instructions.
- If you did not attend the scheduled data collection sessions.
- If the whole project is stopped, for reasons not known now.

Voluntary Participant Data

Name	
Status	
Email	
Telephone	
Fax	

Responsible for the Selection of Voluntary Participants



<i>Name</i>	
<i>Address</i>	
<i>Email</i>	
<i>Telephone</i>	
<i>Fax</i>	
Exercise details	
<i>Exercise Plan Form</i>	(Id number)
<i>Actor Role Form</i>	(Id number)
<i>Applicable Laws/Directives</i>	
<i>Date</i>	(dd/mm/yy)
<i>Declaration</i>	I have read the terms outlined and understand them. I consent to the terms <i>Signature</i>

5.1.11 Ethical standards for research

The consortium and the Coordinator in particular, commit to upholding the highest ethical standards for research, as delineated in the **European Code of Conduct for Research Integrity** of ALLEA (All European Academies) and ESF (European Science Foundation) of March 2011, which states specifically:

“Researchers, public and private research organisation, universities and funding organisation must observe and promote the principles of integrity in scientific and scholarly research. These principles include:

honesty in communication; reliability in performing research; objectivity; impartiality and independence; openness and accessibility; duty of care; fairness in providing references and citing appropriately; and responsibility for the scientists and researchers of the future”.

5.1.12 Ethics Self-Assessment

We hereby state that we have not identified any issues with regards to informed consent, or use of sensitive personal data. Non-sensitive personal data collection is envisioned through workshops, questionnaires and interviews and sufficient controls are applied to guarantee data protection and privacy of participants. Furthermore, during the course of carrying out the work in PERSONA, the nature of the research means that:

- The planned research will not involve persons unable to give informed consent;
- The planned research will not involve vulnerable individuals and groups;



- The planned research will not involve children or minors;
- The planned research will not involve the collection or processing of sensitive personal data (e.g. health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction).
- There is no plan to import any material including personal data from non-EU countries
- All data which is not provided by the project partners or associate partners and which will be used in the project is publicly available;
- While implementing the work described in the technical annex, the ethical standards are guidelines of Horizon 2020 will be strictly adhered within, regardless of the country in which the research is carried out.
- No materials or personal data from members of the public or employees of the different organisation involved in the project and requiring authorisations for transmission will be imported or exported from the EU during the implementation of the project.

Section 1: Human Embryos/Foetuses	Yes/No		Page	Information to be provided	Documents to be provided
Does your research involve Human Embryonic Stem Cells (hESCs)?		X			
Does your research involve the use of human embryos?		X			
Does your research involve the use of human foetal tissues/cells?		X			
Section 2: Humans	Yes/No		Page	Information to be provided	Documents to be provided
Does your research involve human participants	X				
Does your research involve physical interventions on the Study participants		X			
Section 3: Human Cells/Tissues	Yes/No		Page	Information to be provided	Documents to be provided
Does your research involve human cells or tissues (other than from Human Embryos/Foetuses, see Section 1)		X			
Section 4: Protection of Personal Data	Yes/No		Page	Information to be provided	Documents to be provided
Does your research involve personal data collection and/or processing	X				

Does your research involve further processing of previously collected personal data ('secondary use') (including use of per-existing data sets or sources, merging existing data sets, sharing data with non-EU member states)?	X				
Section 5: Animals	Yes/No	Page	Information to be provided	Documents to be provided	
Does your research involve animals?		X			
Does your research involve research procedures that may cause pain; suffering; distress or lasting harm to live non-human vertebrate animals (including independently feeding larval forms, foetal forms of mammals in the last trimester of their normal development and cephalopods)?		X			
Section 6: Third Countries	Yes/No	Page	Information to be provided	Documents to be provided	
Does your research involve third countries?		X			
Are research activities going to be carried out in third country? Specify the countries involved		X			
Do you plan to use local resources (e.g. animal and/or human tissue samples, genetic material, live animals, human remains, materials of historical value, endangered fauna or flora samples, traditional knowledge, etc.)?		X			
Do you plan to import any material from third countries into the EU? For data imports see Section 4 For imports on human cells or tissues, see Section 3		X			
Do you plan to export any material from the EU to third countries? For data export, see Section 4		X			
If your research involves low and/or lower-middle income countries, are any benefit-sharing plans planned?		X			

Could the situation in the country put the individuals taking part in the research at risk?		X			
Section 7: Environment & Health and Safety	Yes/No		Page	Information to be provided	Documents to be provided
Does your research involve the use of elements that may cause harm to the environment, animals or plants? For research involving animal experiments, see Section 5		X			
Does your research deal with endangered fauna and/or flora/protected areas?		X			
Does your research involve the use of elements that may cause harm to humans, including research staff? For research involving human participants see Section 2		X			
Section 8: Dual Use	Yes/No		Page	Information to be provided	Documents to be provided
Does your research have the potential for military applications?		X			
Section 9: Misuse	Yes/No		Page	Information to be provided	Documents to be provided
Does your research have the potential for malevolent/criminal/terrorist abuse?		X			
Section 10: Other Ethics Issue	Yes/No		Page	Information to be provided	Documents to be provided
Are there any other ethics issues that should be taken into consideration? Please specify		X			

5.2 Societal Impact

By essence, like for any proposal of the Secure Societies call, the developments proposed address threats to society and the objective of PERSONA is obviously to enhance its resilience; this is



especially the case here, as the objective of PERSONA is to create a new generation of law enforcement agents, called Special Cognitive Forces, equipped with efficient computational and communicational system.

PERSONA will address in depth the societal trade-offs associated to the implementation of the different proposed measures through a dedicated WP: WP2 “Ethical, Privacy and Security of PERSONA Platform”, led by the Norwegian Crime Police, which is specialized in this domain.

6 Security

Please indicate if your project will involve:

- activities or results raising security issues: NO
- 'EU-classified information' as background or results: NO

Even if it is not foreseen the PERSONA project will utilise or create EU-classified information, the project will monitor security criticality of the technical system and the pilot execution through the management team, a Security Advisory Board and with the support of the External Advisory Members, including experts in Security. About the details of the composition and functioning of the boards, read Task 5.1. In case of security criticality will be raised, the project consortium chaired by the Project Coordinator will suggest appropriate procedures to resolve the same.