PERSONA Deliverable D3.1: PERSONA assessment method (initial version)

Casiraghi, Simone; Kloza, Dariusz; Konstantinou, Ioulia; Calvi, Alessandra; Burgess, James Peter

Publication date:
2020

Document Version:
Final published version

Privacy, Ethical, Regulatory and SOcial
No-gate crossing point solutions Acceptance

D3.1: PERSONA assessment method (initial version)

WP3: Assessment method and orchestration framework development

Lead beneficiary: VUB

Delivery date: May 2020

Dissemination level: Public

Project title: PERSONA - Privacy, Ethical, Regulatory and SOcial No-gate crossing point solutions Acceptance
Duration: 1 September 2018 - 28 February 2021

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 787123.

Document information

Document status	
Document lead	Simone Casiraghi, Dariusz Kloza, Ioulia Konstantinou, Alessandra Calvi, James Peter Burgess (VUB)
Internal reviewer	José-Ramón Martinez (ATOS) Paulo Chaves (INOV)
Type	Report
Work Package	WP3: Assessment method and orchestration framework development
Task(s)	T3.1: Research method for acceptance assessment
Deliverable number and title	D3.1: PERSONA assessment method (initial version)
Due date	M12, August 2019
Delivery date	06 May 2020
Distribution	PERSONA consortium, European Commission

Document history	
Versions	*v0.1 VUB, 02/08/2019, definition of table of contents* *v0.2 VUB, 19/08/2019, chapter 1 and draft of checklist* *v0.7 VUB, 23/08/2019, draft chapter 2 and 3* *v0.8 VUB, 26/08/2019, first complete draft for contributions* *v0.9 CEL, SPA, PRIO, RISE, 27/08/2019, draft with comments* *v1.2 VUB,28/08/2019 version for internal reviewers (ATOS and INOV)* *v1.3 VUB, 29/08/2019 integration of ATOS and INOV comments* *v1.4 VUB, 30/08/2019, final proofreading and editing* *v1.5 VUB, 30/08/2019, final version* *v1.6 VUB, 06/05/2020, change dissemination level*
Contributions	CEL: Antonio Carnevale, Maria Pia Verzillo; section on social acceptance and comments on the document.
	PRIO: Kristoffer Lidén; comments on the document.
	ATOS, INOV: internal review of the document
	VUB: draft of the document, incorporation of comments by reviewers.

Project partners

Logo	Partner	Country	Short
	Vrije Universiteit Brussel	Belgium	VUB
	Institutt for Fredsforskning Stiftelse	Norway	PRIO
	Cyberethics Lab Srl	Italy	CEL
	Atos Spain Sa	Spain	ATOS
	Inov Inesc Inovacao – Instituto de Novas Tecnologias	Portugal	INOV
	Queen Mary University Of London	UK	QMUL
	Polismyndigheten Swedish Police Authority	Sweden	SPA
	Bundesrechenzentrum Gmbh	Austria	BRZ
	Ministarstvo Unutrasnjih Poslova Republike Srbije	Serbia	SMOI
	Ministry of Public Security	Israel	MOPS-INP
	RISE Research Institutes of Sweden	Sweden	RISE

Project website

http://www.persona-project.eu

List of abbreviations

CBA	Cost-Benefit Analysis
CoS	Community of Stakeholders
DoA	Description of the Action
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
Dx.y.	Deliverable
EAB	External Advisory Board
eIA	Ethical Impact Assessment
EIA	Environmental Impact Assessment
EUDPR	Data Protection Regulation for EU Institutions
GDPR	General Data Protection Regulation
IA	Impact Assessment
IIA	Integrated Impact Assessment
LEA	Law Enforcement Authority
LED	Law Enforcement Directive
NGO	Non-Governmental Organisation
PIA	Privacy Impact Assessment
SWOT	Strengths, Weaknesses, Opportunities and Threats
TA	Technology Assessment
WP	Work Package

Executive summary

Deliverable D3.1 contains the first version of the integrated impact assessment (IIA) method for the PERSONA project. Such a method is a step by step iterative process to be applied in order to assess the impact of borderless crossing technologies against the legal requirements and ethical and social acceptability issues identified in the benchmark (D1.3). This version of the method will be updated and improved in D3.2 (*PERSONA assessment method – final version*). Both Deliverables D3.1 and D3.2 constitute a tailor-made integrated impact assessment that will be included in the final textbook of the project (D5.3).

Table of contents

1 Introduction

1.1 General introduction

Deliverable D3.1 introduces the notion of "impact assessment" (IA) for the PERSONA project. It elaborates an initial version of a tailor-made integrated method that law enforcement authorities (LEAs) and governments could use whenever they take a borderless crossing initiative, or implement a new technological device or system, to ensure the legal requirements and the ethical and social acceptability measures are met.

In line with both literature and established practices on integrated impact assessments (IIA), the deliverable deals with what should be the constitutive elements of the impact assessment method for borderless crossing technologies. There is no "one-size-fits all" model for these processes and in general, their steps and techniques are tailored based on the specific scope of each assessment exercise.

The method elaborated in this deliverable identifies the scope of the assessment against a specific "benchmark" (outlined in D1.3). This is why the deliverable is strictly correlated to D1.3 which identifies a list of issues and requirements stemming from the legal, ethical and societal principles that apply to PERSONA and, by extension, borderless crossing initiatives in general.

Deliverable D3.1 consists of five chapters (plus bibliography):

Chapter 1 introduces the concept of impact assessment and its vocabulary in the context of the PERSONA project. This will include an explanation of the concept of method, framework and integrated impact assessment (IIA), as well as a generic method for impact assessment, that will be tailored down in the subsequent sections.

Chapter 2 describes, from a theoretical perspective, which parts of the generic method need to be tailored down to the context of border control, as well as why and how this should be done.

Chapter 3 aims to operationalize the method and its steps provided in section 2 and offers a clear guidance to the assessor on how to conduct the IIA process.

Chapter 4 contains some questions that can be used by the assessor at specific points of the IIA process as a checklist, plus a table with milestones to ensure the goals of each objective are achieved.

Chapter 5 contains concluding remarks and sketches the future development of the IIA method in the project.

It is important to note that this deliverable includes an initial version of the method, which will be further updated in D3.2, due in M24.

1.2 Architecture & IA vocabulary

1.2.1 Vocabulary

The 'architecture' for impact assessment typically consists of two main elements, which are called here 'framework' and 'method'. These are supplemented by e.g. guidelines, templates or questionnaires. A *framework* constitutes an "essential supporting structure" or organisational arrangement for something, which, in this context, concerns the policy for impact assessment, and defines and

describes the structure, principles and rules thereof. In turn, a *method*, which is a "particular procedure for accomplishing or approaching something", concerns the practice of impact assessment and defines the consecutive and/or iterative steps to be undertaken to perform such a process in accordance with the framework. A method can be generic or it might be tailored down to a specific context.

There already exist multiple frameworks and methods for impact assessment in many domains of practice, of various applicability and – more importantly – quality. A constant need for new ones is a function of the principle of receptiveness of impact assessment, i.e. both framework and method are to be continuously improved for impact assessment to better serve its goals, by learning from previous experience, their own or of other evaluation techniques; to better respond to societal change; or to give effect to new types or domains of impact assessment (e.g. a recently proposed 'algorithmic impact assessment').[1] Each new and revised framework and method is meant to contribute towards the efficiency (i.e. effectiveness with the least waste of resources), integrity (completeness) and fairness (legitimacy, impartiality and balance) of the assessment process so that the assessment process better serves its goals, i.e. the protection of a given societal concern, or concerns, among others.[2]

The integrated method offered in this deliverable is built on the research carried out in the project PERSONA, and on the experience of its partners in various domains of practice of impact assessment, in particular those of privacy, personal data protection (informational privacy), technology development, environmental protection and human rights. Nevertheless, given the principle of receptiveness of impact assessment, the method needs to be periodically revised as the experience of their use grows and the society changes. Accordingly, a subsequent version of the present method will be developed in D3.2 (due M24).

1.2.2 Framework

The tool of impact assessment, in general, is governed by a set of principles, i.e. a framework, built on best practices in different established areas of practice, such as technology assessment (TA), environmental impact assessment (EIA) and privacy impact assessment (PIA). These principles can be summarised as follows and are equally applicable to the process of impact assessment in the PERSONA project:[3]

1. The impact assessment is a systematic process, undertaken in accordance with an appropriate method, and conducted in a timely manner. It starts reasonably early in the lifecycle of a single initiative, or a few alike initiatives (e.g. a proposed technology or a piece of legislation), prior to their deployment, continues throughout its life cycle and – as the society changes, dangers evolve and knowledge grows – is revisited when needed (a 'living instrument'), thus continuously influencing the design of the initiative under assessment.
2. Impact assessments analyse possible consequences of an initiative against the relevant societal concerns, both individual and collective, commensurate with its type (e.g. DPIA is about the protection of individuals whenever their personal data are being processed and EIA – natural and human environment). Threshold analysis (scoping, establishing the context), public participation and expert consultation help determining and keeping up-to-date the list of these concerns. Whenever necessary, multiple types of impact assessments are performed for a given initiative, possibly in an integrated way.

[1] Based on: (Kloza et al., 2017)
[2] Based on: (Kloza et al., 2019)
[3] Based on: (Kloza et al., 2017)

3. Not all initiatives require impact assessments. The need is therefore determined by factors such as the nature, scope, context and purpose of the initiative under assessment, the number and types of individuals affected, etc. Impact assessments are however compulsory at least for initiatives capable of causing severe negative consequences to relevant societal concerns.
4. 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. These methods can range from qualitative or quantitative risk management, to scenario planning, to scientific foresight, supported by a compliance check with relevant legal and otherwise regulatory requirements (e.g. technical standards).
5. The impact assessment process not only identifies, describes and analyses possible consequences – positive or negative, intended or unintended – of an initiative under assessment, but also identifies, describes and analyses possible solutions (recommendations) to address these consequences.
6. Impact assessments constitute 'best efforts obligations'. Since it is impossible to reduce negative consequences in absolute terms (and maximise positive ones), organisations react to them to the best of their abilities, depending upon the state-of-the-art and, to a reasonable extent, available resources.
7. The impact assessment process requires the assessor, or a team of assessors, to have sufficient knowledge and know-how for its successful completion, corresponding to the type of impact assessment at stake.
8. The impact assessment process is documented (in particular, in writing) and is reasonably transparent. Its transparency manifests itself in free (i.e. unrestricted) and public access to relevant information. The public at large is informed about the assessment process, its terms of reference (in particular, the method) and its progress. Both draft and final assessment reports are easily accessible. This is without prejudice to legitimate secrecy.
9. The impact assessment process is deliberative, manifested predominantly by public participation. External stakeholders – be it individuals and/or civil society organisations concerned or affected by the initiative under assessment), as representative as possible – are identified and meaningfully informed about it, their voice is actively sought and duly taken into consideration (i.e. consultation and co-decision). Information given and sought is robust, accurate and inclusive. Individuals and/or their representatives have effective means of challenge, e.g. in a court of law or similar tribunal. In parallel, anyone within the organisation sponsoring the initiative under assessment (i.e. internal stakeholders) partakes in the assessment process under the same conditions. Exceptions to public participation, if justified, are interpreted narrowly.
10. An organisation sponsoring an initiative is accountable for the impact assessment process. Decision-makers within an organisation choose, *inter alia*, the method of assessment and assessors to conduct it. They eventually approve the final impact assessment report and subsequently monitor the implementation of proposed possible solutions (recommendations). An external entity (e.g. a regulatory authority or an audit body) scrutinises its quality; selection criteria are transparent. Therefore, an organisation is able to demonstrate the satisfactoriness of the undertaken impact assessment process. Whenever impact assessments are compulsory, non-compliance and malpractice are proportionately sanctioned.
11. The independence of the assessor – be it external or in-house – is ensured: they do not seek nor accept any instructions, and have sufficient resources (i.e. time, money, manpower, knowledge and know-how, premises, and infrastructure) at their disposal.
12. The impact assessment process is sufficiently simple, i.e. not unduly burdensome. The method

serves those who use it and therefore is structured, coherent, easily understandable, and avoids prescriptiveness, over-complication and abuse of resources. There is an inherent trade-off between the simplicity of use, and the technical sophistication and accuracy of the assessment.

13. The impact assessment process is adaptive to the characteristics of an initiative under assessment and its sponsoring organisation (i.e. 'one size does not fit all'), e.g. type and complexity thereof (e.g. technology development, scientific research, legislative proposals) or the type and number of individuals concerned (affected) (e.g. nuclear safety is not the same as personal data protection). It can be connected with impact assessments in other areas, if possible. It is responsive to geographical and cultural differences.
14. The impact assessment process is inclusive. This ensures as many stakeholders, relevant societal concerns and relevant development phases as possible (i.e. both the initiative under assessment and the process leading thereto), commensurate with the societal concerns at stake and the type of assessment, are included in the assessment process. It bases its analysis on both expert and layperson knowledge (i.e. public participation).
15. The impact assessment is receptive. Both the method and the process evolve by learning from previous experience in parallel evaluation techniques (e.g. TA, EIA, risk management, etc.), knowledge from related disciplines (e.g. law), and changes in the society.
16. Impact assessments require a supportive environment to bear fruit. They need continuous high-level support from policy- and decision-makers and a spirit of cooperation among external and internal stakeholders. Regulators offer guidance and practical assistance in the assessment process, in the form of adequate training, guidelines, explanations and advice.

1.3 A generic method for impact assessment

The generic method for impact assessment consists of the following ten steps (six consecutive steps, three executed throughout the entire process and one step conducted afterwards), grouped in five phases. The said method is built on best practices in different established areas of practice and reflects the above-mentioned 16-principle framework.[4]

Phase I: Preparation of the assessment process

1) *Screening (threshold analysis)*. A step to determine whether the process of impact assessment is warranted or necessary for a planned initiative under assessment, or a set of similar initiatives, and in a given context. The screening is based on an initial yet sufficiently detailed description of the said initiative, both contextual and technical. The determination is made in accordance with threshold criteria, both internal (i.e. organisation's own policies) and external (i.e. set forth by legal or otherwise regulatory requirements), or *ad hoc* criteria, e.g. due to the pressure of the public opinion. In case the conduct of the assessment process is neither warranted nor necessary, the entire process is then concluded by a reasoned statement of no significant impact.
2) *Scoping*. A step, based on the initial description, to identify:
   a) a societal concern, or concerns, which a planned initiative might touch upon, e.g. privacy, personal data, applied ethics, natural and human environment, as well as the corresponding legal or otherwise regulatory requirements;
   b) stakeholders who might affect, be affected, concerned by or interested in the envisaged

[4] Based on: (Kloza et al., 2019)

initiative(s), or who possess knowledge thereon, as well as the level of their involvement;

c) techniques for the appraisal of impacts and for stakeholder involvement that would be used throughout the assessment process; and

d) other evaluation techniques, beyond the process of impact assessment, to which resorting might be necessary or warranted.

Not all of these elements and people might be identifiable at the beginning of the assessment process and hence their identification might need to be revised periodically.

3) *Planning and preparation*. A step to define the terms of reference for conducting the assessment process. These include, among others, the objectives thereof, the criteria of acceptability of negative impacts, the necessary resources (i.e. time, money, manpower, knowledge, know-how, premises and infrastructure), the procedures and time-frames of the assessment process, the assessor or the team of assessors (in-house or outsourced) and their roles and responsibilities, as well as the continuity of the assessment process.

Phase II: Assessment

4) *Description*. A step, based on the initial description (cf. Step 1), to provide a detailed, two-partite account of the planned initiative. First, a contextual description typically consists of (a) an overview of the planned initiative(s) and of the sponsoring organisation, (b) context of its deployment, (c) the need therefor, (d) possible interference(s) with societal concern(s), and (e) expected benefits and drawbacks. Second, a technical description consists of e.g. – in case of DPIA – inventories of categories of personal data and their flows.

5) *Appraisal of impacts*. A step in which the impacts of the envisaged initiative are appraised in accordance with pre-selected techniques. Typically, such appraisal consists of – at least – identification, analysis and evaluation of impacts. Appraisal techniques could range from risk analysis (qualitative, quantitative risk management, or a combination of both), scenario analysis (planning), technology foresight; to legal and regulatory compliance check, proportionality and necessity tests; to the cost-benefit analysis (CBA) and the strengths, weaknesses, opportunities and threats (SWOT) analysis.

Phase III: Recommendations

6) *Recommendations*. A step in which concrete, detailed measures (controls, safeguards, solutions, etc.), their addressees and time-frames are proposed to minimise negative consequences of a planned initiative and, if possible, to maximise positive ones; both 'negative' and 'positive' are subjective concepts. Prior to their determination, the assessor takes stock of the controls already implemented. Assessor might suggest also impacts whose treatment might be prioritised. On such a basis, after the conclusion of the assessment process, the leadership of a sponsoring organisation takes a decision as to the deployment of an initiative and conditions therefor. An initiative might be cancelled altogether if the consequences would be unacceptable.

Phase IV: On-going steps

7) *Stakeholder involvement (public participation) in decision-making*. A step in which stakeholders and/or their representatives take part in the assessment process. Having been identified, their level of involvement can range from: (a) merely being informed about a planned initiative or educated thereon (low level); (b) dialogue and consultation, in which their views on the initiative are sought and taken into consideration (middle level); to (c) to co-decision about the deployment of the initiative in question and, subsequently, partnership in its implementation (high level). In case stakeholder involvement is neither warranted nor necessary, such a choice is

reasoned and documented. Stakeholder involvement does not compromise any legitimate secrecy, e.g. state or trade secrets, nor it brings any negative consequences for participants (e.g. exploitation). Legal remedies are available for the absence of stakeholder involvement, or its insufficiency, commensurate to the level of involvement pursued in a given assessment process.

8) *Documentation*. A step in which intelligible records are kept, in writing or in other permanent form, including a register of impacts (risk), about all the activities undertaken during the assessment process. This step includes the preparation of a final report from the assessment process (or a statement of no significant impact, if the assessment process is not warranted or necessary). The full spectrum of documents from a given impact assessment process, preferably in an electronic format, might be made publicly available, presented for inspection upon request, as well as centrally registered.

9) *Quality control of the assessment process*. A step in which the adherence to a standard of performance is checked, internally (e.g. progress monitoring or a review within an organisation) or externally (e.g. by an independent regulatory authority, e.g. audit, or a by court of law), during or after the assessment process, or both.

Phase V: Revisiting

10) *Revisiting*. A step in which a decision is made as to whether to reconduct the assessment process entirely or in part. It can occur every time the envisaged initiative is modified (before or after its deployment) or the context in which it is going to be deployed, or already has been deployed, changes. This step ensures the continuity of the assessment process, e.g. in case of a transfer of the initiative to another organisation.

1.4 "Integrated" impact assessment

Multiple areas (domains) and types of assessment processes could be integrated into a single one. Such integration might be beneficial for at least three reasons: (1) since "everything is inherently interconnected", "a complete understanding of all the impacts can only be achieved by a comprehensive and integrated assessment"[5]; (2) efficiency "in terms of monetary and time resources", and (3) inclusion of the aspects not legally required in the types of assessments that are required by law (i.e. "greater visibility of voluntary impact assessments by piggy-backing on those that are legally mandated").[6]

Such integration would function on a condition that the integrated method, in particular its benchmark, is internally coherent and not contradictory. Moreover, while "integration may contribute to efficiency, it could also lead to the subordination of certain assessment issues, particularly those that are supposed to have their status raised in decision making through specific assessment instruments".[7]

The integrated impact assessment (IIA) of PERSONA combines several assessments and appraisal techniques, which are either legal requirements (e.g. DPIA) or good practices, into one single process. The integration of different types of IA into a single process can help LEAs and border authorities to conduct the assessment in two ways. First, it would improve the efficiency of the process since many issues (e.g. privacy) overlap across different IA. Second, outcomes and recommendations for policy

[5] (Vanclay, 2004) p. 277
[6] (Tajima & Fischer, 2013) p. 29
[7] Ibid.

makers could be simplified. This is in line with the principle of adaptiveness (n. 13) of the aforementioned framework.

An IIA is widely used in the European Union,[8] especially in the UK in cases where environmental, health and social IA are combined to assess the impact of city planning initiatives.[9]

This PERSONA IIA combines the following impact assessments:

- Ethical Impact assessment (eIA), including social acceptance,[10]
- Privacy impact assessment (PIA), and
- Data protection impact assessment (DPIA).

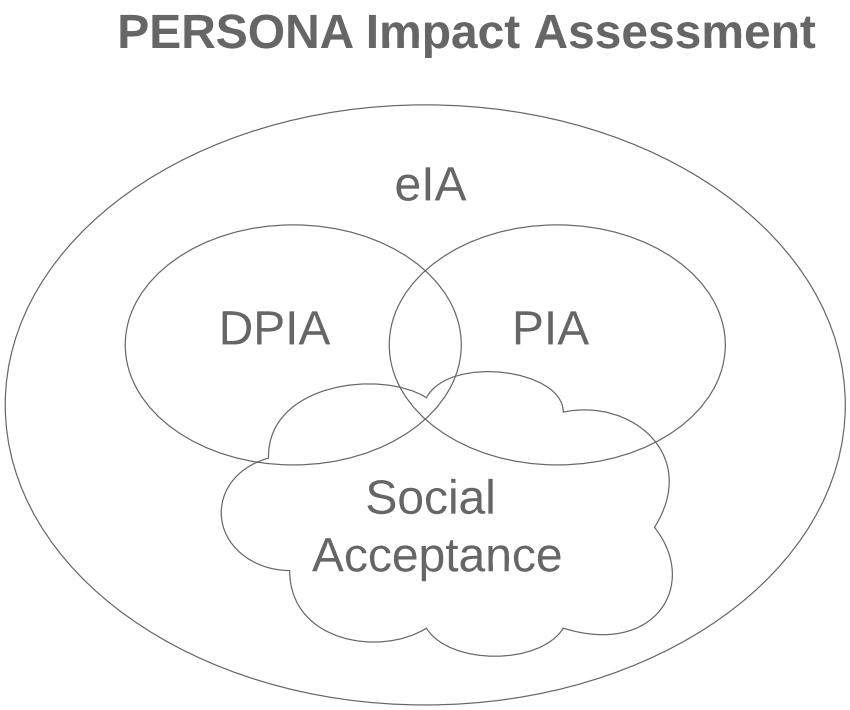

Figure 1: PERSONA Integrated IA components

[8] (Smismans & Minto, 2017)
[9] (London Plan, 2017); (City of Westminster, 2019)
[10] By social acceptance here we do not mean 'social impact assessment'. The concept of social acceptance enquires empirically whether a new technology is accepted—or merely tolerated—by a community (see more on this in D1.3). Social impact assessment instead is a well-established practice that assess the social effects (in a broader sense) of a given initiative. Given the scope of PERSONA, we decided to treat social acceptance as part of the eIA pillar, and not as a separate one like e.g. DPIA.

2 The PERSONA impact assessment method

The generic method for impact assessment needs to be tailored down to the specificity and needs of a given context. While the general captions of section 1.3 will be kept as they are,[11] each step will be tailored down to each component of the PERSONA IIA (DPIA, eIA, PIA) and to the context of border control. This exercise will require two separate steps corresponding to sections 2 and 3 of this deliverable.

- Section 2 deals with the theoretical justification of why, where and how the method needs to be tailored down.
- Section 3 provides concrete step by step guidance for the assessor.

The parts in yellow of the graphic below are useful to visualise which parts of the method need to be tailored down for each type of impact assessment:

Table 1: Tailoring down the generic IA method to the PERSONA IIA components

Steps	DPIA	Ethical IA (including social acceptance)	PIA
Phase I			
1) Screening	-Legally binding -4 iterations: ▪ GDPR: 6 criteria to consider ▪ LED: 1 criterion ▪ EUDPR: 5 criteria to consider ▪ EUDPR: 1 criterion for AFSJ	-Not legally binding -Threshold analysis questionnaire	-Not legally binding -Threshold analysis questionnaire
2) Scoping	-Narrow down the benchmark to relevant legal statutes -Identify appraisal techniques for: ▪ Risk to a right ▪ Necessity and proportionality test	-Narrow down the benchmark to relevant ethical principles -Identify appraisal techniques for ethical issues	-Narrow down the ethical benchmark to relevant privacy issues -Identify appraisal techniques for privacy issues
	-Identify stakeholders -Identify stakeholders involvement techniques		
3) Planning	Determine scale, budget, composition of the team		
Phase II			

[11] This generic method was used to conduct the internal DPIA of the PERSONA project (D8.3) and was discussed during the second roundtable of the first PERSONA workshop (see D6.2).

4) Description	Systematic description of envisaged processing operations [Art 35(7)(a) GDPR & Art. 39(7)(a) EUDPR] Or Generic description of envisaged processing operations (LED & Art. 89 EUDPR) And Technical description of processing operation	Broader 'big picture' description of the initiative (relevant ethical, privacy and societal issues not covered by data protection)	
5) Appraisal of impacts	Necessity & Proportionality + Risk assessment (GDPR & Art. 39 EUDPR) Risk assessment (LED and Art. 89 EUDPR)	-Applied Ethics -Ethical Checklist approaches -Participatory methods -Stakeholders consultation -Scenario-based approaches	-Risk assessment -Cost-benefit analysis (CBA)
Phase III			
6) Recommendations	Measures envisaged to address the risks AND demonstrate compliance with data protection rules	Broader scope recommendations that do not fall under data protection recommendations	
Phase IV (on going)			
7) Stakeholder involvement	Identify, define the level of involvement and Involve stakeholders at different phases of the process		
8) Documentation	Document the IA process		
9) Quality control	Check the quality of the IA process (internally or externally)		
10) Revisiting	Revise the IA process		

2.1 Phase I: Preparation of the assessment process

2.1.1 Screening (threshold analysis)

Each initiative presents its own peculiarities and that is why the threshold has different requirements in DPIA, eIA and PIA. To begin with, it is important to determine whether any IA is required by the law. At the moment of writing, the only types of impact assessment required under EU law, are the data

protection (DPIA) and environmental (EIA) ones. As EIA falls out the scope of this project, we begin by discussing the threshold analysis of DPIAs.

a) At DPIA level, there are differences between the DPIA foreseen under the General Data Protection Regulation (GDPR) in Art. 35, under the Law Enforcement Directive (LED) in Art. 27 and under the so-called General Data Protection Regulation for EU Institutions (EUDPR), which in turn distinguish DPIA carried out by Union bodies, offices and agencies when carrying out activities which fall within the scope of Chapter 4 (Judicial cooperation in criminal matters) or Chapter (Police cooperation in criminal matters) 5 of Title V (Area of Freedom, Security and Justice) of part three TFEU data (Art. 89) and DPIA carried out in the other policy areas (Art. 39). Furthermore, whereas a matter falls entirely within national security, it is outside the scope of EU law and none of the above legal framework will be applicable.

   That is why it is necessary for the data controllers to understand in which policy area they are operating, even if the lines may be blurred Nevertheless, there may be situations of overlap and changes.

   > A person crossing the Schengen borders irregularly might be checked by a police officer and, in those Member States where the irregular crossing of borders qualifies as a criminal offence, the police officer may change the purpose of the processing, depending on whether it is carried out for migration purposes or for prosecuting the criminal offence. However, once the irregular migrant applies for asylum, the processing of his application will fall within the scope of the GDPR, notwithstanding the initiated criminal proceedings.[12]

   Under the GDPR, in order to determine whether a process of DPIA is required by law, the envisaged initiative has to be examined against the six criteria of **high risk** (to the rights and freedoms of data subjects, taking into account four qualitative criteria of the nature, scope, context and purposes of the processing of personal data), **enumeration** [list in Art. 35(3)], **positive enumeration** by data protection authorities (DPAs), **negative enumeration** by DPAs, **selected previous assessment processes**, **exemptions for specific professions** (see Section 3 for further details).

   In the LED, the formulation Art. 27 is simpler: the only criterion mentioned is to have processing operations likely to present **high risk** to the rights and freedoms of data subjects, taking into account four qualitative criteria of the nature, scope, context and purposes of the processing of personal data.

   In the EUDPR, the structure of Art. 39 and 89 retrace that one of Art. 35 GDPR and Art. 27 LED respectively, *mutatis mutandis* (e.g. positive and negative enumeration lists are adopted by the European Data Protection Supervisor, and there is no exemption for specific professions).

   Data processing operations involving new technologies constitute a particular trigger for all the above DPIAs.

b) Nevertheless, other types of impact assessment, albeit not required by law may still be desirable. As for ethical impact assessment (eIA), it might still be needed for a given border control initiative if the severity of the possible ethical impacts is high. As there are no explicit criteria provided by the law, it is up to the assessor to determine whether the threshold to conduct an ethical impact assessment is met. However, the determination of the threshold is necessary only if a DPIA is not required by law. In fact, serious concerns about data protection

[12] (Sajfert & Quintel, 2019)

issues and risks to rights and freedoms of data subjects are also ethical matters, and thus require an eIA. Only if a DPIA is not required then an assessor is requested to perform a threshold analysis. In order to take this decision, the assessor could, for instance, fill in a threshold analysis questionnaire (self-assessment), where quantitative criteria (e.g. a numerical scale) could indicate whether the threshold is met. As a rule of thumb, if any ethical issue is raised by the project (including, but not limited to, data protection issues), an eIA should be conducted. If no threshold is met (i.e. no potential ethical issues are raised), an independent body (e.g. data protection authority for what concerns a DPIA, internal ethics committees or external advisory boards for ethics) should review the assessment form to ensure that this is the case.

Finally, if ethical impacts concern specifically the field of privacy (including bodily, informational, spatial privacy etc.),[13] a PIA might be warranted. This could create a situation where a DPIA is not carried out, while a PIA is undertaken. In fact, while people still confuse the two, privacy and data protection are indeed two different rights and theoretical concepts, and there may still be situations where privacy is affected independently from personal data processing (interception of telecommunications)[14]. According to Wright and De Hert, there are at least two ways to address the question of whether a PIA is necessary. First, it should ask whether the project involves the processing of personal data or could impact any type of privacy, i.e. whereas a DPIA is required, also a PIA should be recommended. Second, it should contemplate what could go wrong in relation with one project and see if there are some privacy risks. Furthermore, Clarke suggests considering if the proposed project has significant potential impacts on, or implications for, groups of people or organisations other than the primary sponsor (e.g. in case of databases).[15]

In sum, it is important to conclude that, in a given initiative, it might be the case that not all the pillars of the IIA are needed. For instance, it might be the case that a DPIA is not required by law, but still an eIA and/or PIA should be conducted.

2.1.2 Scoping

As for the scoping phase, the five main steps of the scoping are to preliminary identify:

a) The level of granularity of the initiative under assessment. The assessment process (and its scale) will look very different if for 'initiative' it is meant, say, a component of the technology (e.g. a fingerprint reader for a smart gate), or a complex system/assemblage that integrates several devices (e.g. a smart tunnel that includes face recognition cameras, sensors and body scanners). It is also important to determine where this initiative will be implemented: is it one single device used in a pilot at a single airport? Or at multiple border crossing points?

b) A societal concern, or concerns, which a planned initiative might touch upon, i.e. privacy, personal data protection, applied ethics or other rights and freedoms. To do this, the assessor should use the benchmark developed in D1.3 as a guidance, but she needs to narrow it down to the specific context (e.g. a body scanner or a facial recognition system, etc.), in particular regarding:

   a. Technical requirements that apply to the initiative under assessment (including functional, non-functional and security requirements) (see D1.1 as an example);

[13] For a complete typology of privacy see (Koops et al., 2017)
[14] (Kokott & Sobotta, 2013)
[15] (Wright & De Hert, 2012) p. 46

b. Legal statutes regarding border management that apply to the given initiative;

c. Ethical principles that apply to the given initiative;

d. Legal principles that apply to the given initiative.

It is important that the elements selected from the benchmark are consistent: there should be no contradictions e.g. between legal requirements on border control (a) and legal principles of privacy and data protection (d), or between functional requirements of the system (a) and ethical principles (c). It is also important to take into account the technical requirements of the system; sometimes the outcome of the assessment might be too negative because the assessor thinks the technology is capable of doing more than it actually does, or the error rate is very high (think of the case of a facial recognition system).

c) stakeholders who might affect, be affected, concerned by or interested in the envisaged initiative(s), or who possess knowledge thereon, or their representatives, as well as the level of their involvement. The identification of stakeholders is highly depended on the context, but can be done once for each component of the IIA. For instance, in the context of lie detection systems applied at border crossing points, the stakeholders will be, other than by border control authorities and other law enforcement authorities, companies developing the systems, represented by travellers. In turn, the category of travellers can be divided into various subsets with various needs: there are business travellers, family travellers, elderly people travelling, children, people with disabilities whose needs have to be taken into account.

d) techniques for the appraisal of impacts and for stakeholder involvement that would be used throughout the assessment process. In DPIA, for example, the appraisal techniques are necessity and proportionality and high risk (for Art. 35 GDPR and Art. 39 EUDPR) and high risk in Art. 27 LED and Art. 89 EUDPR. However, resort to other appraisal techniques for ethical impact might be necessary.

e) other evaluation techniques, beyond the process of the present impact assessment, to which resorting might be necessary or warranted. For instance, it could be required to do a Health Impact Assessment (HIA), for instance in the case of particular types of body scanners which employ millimetre wave radiation.[16]

Not all of these elements and people might be identifiable at the beginning of the assessment process and hence their identification might need to be revised periodically.

2.1.3 Planning

It is very important to timely organize the planning of the IIA process, as this might be very resource consuming in terms of money, effort and time. This step aims to determine:

a) The scale of the assessment (small-medium-large). This will depend on the type of technology assessed (e.g. a single component of a technology e.g. a new fingerprint reader in a smart gate; a single device e.g. a new smart gate; or an integrated complex system, e.g. a smart tunnel) but also on the areas where these technologies are deployed (e.g. a single gate; a whole airport; multiple airports). To determine the scale of the assessment the following guide can be used:

- **Small scale**: one or two ethical issues in the questionnaires above and/or single component or single device assessed

[16] (Valkenburg & van der Ploeg, 2015)

- **Medium scale:** 3-4 ethical issues in the questionnaire above and and/or single component or single device assessed
- **Large scale**: more than 4 ethical issues in the questionnaire above and/or an integrated or complex system to be assessed

b) The budget of the assessment (roughly from 14 000 to 150 000 euro)

c) The time-span of the assessment (roughly from 20 to 60 days) [17]

d) The composition of the team (depending on which pillars of the IIA are considered and on the scale of the assessment). The team conducting the assessment should be as independent as possible from the team working on the implementation of the borderless solution. Being a member of the team requires a sufficient knowledge of the technical aspects of the initiative too, as well as strong knowledge of impact assessment methods, data protection law and/or applied ethics. The team should contain at least:

- Data protection expert(s)
- Lawyer(s)
- Compliance officer
- Ethicist
- Computer security expert
- Border management officers

Besides the composition of the team, an advice from external experts shall be sought. For DPIA, the advice of the data protection officer (DPO), when designated, shall be sought pursuant to Art. 35(2) GDPR and Art. 39(2) EUDPR when carrying out a DPIA. In case of DPIA *ex* Art. 27 LED, the DPO shall provide advice and monitor its performance where requested (Art. 34 LED). In case of DPIA ex Art. 89 EUDPR, there are no provisions on the role of DPO, but *per analogiam* we suggest applying the same provision as in Art. 34 LED, *mutatis mutandis*.

2.2 Phase II: Assessment

2.2.1 Description

The Regulation requires the assessment process to commence with a "systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller" [Article 35(7)(a)]. Such a description necessarily includes:

a) a contextual description of the envisaged initiative, in particular the "nature, scope, context and purposes" of processing operations and stakeholders involved (data subjects, controllers, processors, third parties and public authorities);

b) technical description, containing personal data flows and – possibly – a visualization thereof.

Art. 39(7)(a) EUDPR requires the same (except from the indication of the legitimate interest pursued

[17] It is very difficult to estimate the cost and time of an IIA. This estimation is based on the calculation done by the European Commission in the impact assessment accompanying the GDPR and LED proposals concerning DPIA [Commission Staff Working Paper SEC(2012) 72 final, pp. 124-126]

by the controller).In case of Art. 27 LED and Art. 89 EUDPR, instead, the DPIA shall contain at least a general description of the envisaged processing operations (plus the technical description).

In eIA and PIA, the description should include a broad, "big picture" description of the project, including: the project's overall aims; how these aims fit with the organisation's broader objectives; the project's scope and extent; any links with existing programs or other projects; the key privacy elements. This broader description is necessary only if the impacts of the initiative assessed go beyond data protection related issues, and therefore the description required by the GDPR is not exhaustive for the scope of the IIA.

2.2.2 Appraisal of impacts

The appraisal of impacts has to be done at different levels. If a DPIA is required, then, according to Art. 35(7) GDPR and under Art. 39(7) EUDPR, two types of appraisal techniques have to be performed:

a) necessity and proportionality test, and

b) risk appraisal.

a) The assessment of the "necessity and proportionality of the processing operations in relation to the purposes" of these operations [Article 35(7)(b)]. The distinction between these two concepts and their contents are highly disputable. Nonetheless, in the context of DPIA, this assessment can occur at two levels.

   i. *Level 1 – necessity and proportionality in data protection law:* At the first level, the necessity and proportionality assessment refers to the observance of the personal data protection principles. In particular, it concerns the principle of purpose limitation – i.e. there is a need to assess whether personal data would be "collected for specified, explicit and legitimate purposes and not further processed" inconsistently [Article 5(1)(b)]. This assessment further concerns the principles of data minimisation, accuracy and storage limitation – i.e. whether personal data to be processed would be "adequate, relevant and limited to what is necessary in relation to the purposes", whether they would be "accurate and, where necessary, kept up to date" and whether they would not be stored for longer than necessary [Articles 5(1)(c)-(e)].

   ii. *Level* 2 – *necessity and proportionality in human rights law*: At the second level, the necessity and proportionality assessment refers to human rights limitation criteria. This level is a subsidiary one, triggered only when the first level proves insufficient. It is based on the assumption that the data protection principles are in line with the limitation criteria foreseen in the Charter of the Fundamental Rights of the EU (CFR), read in conjunction with the European Convention on Human Rights (ECHR). Simplifying, any limitation of a non-absolute human right or a freedom, in order to be permitted, must satisfy the criteria of legality, necessity and proportionality, legitimacy, and also must respect for the essence of the right [Article 52 CFR]. This level considers all human rights and freedoms possibly affected by a data processing operation.

   On the grounds of human rights law, a data processing operation is deemed "necessary in a democratic society" when it is undertaken, in the public sector, in response to a "pressing social need" and is "proportionate to the legitimate aim pursued". This entails the consideration of aspects such as the interest(s) at stake (e.g. public safety, public security, freedom to conduct business). For the private sector, in turn, the necessity test entails an examination of economic criteria, e.g. competitiveness or profit. The necessity test further addresses the difference between appropriateness and effectiveness of a processing

operation: while several measures might be appropriate to attains certain objective, they might still not be effective for that purpose.

To be deemed proportionate, on the grounds of human rights law, in turn, a data processing operation – having had its necessity tested – has typically to be capable of ever achieving a legitimate aim (suitability), has to be necessary to that end (necessity) and any less restrictive means must be, reasonably speaking, unsuitable to achieve this aim (proportionality *sensu stricto*).

Both tests – necessity and proportionality – are determined on the basis of fact-based analysis, based on sufficient, clearly described and verifiable evidence. The assessment of necessity precedes its proportionality counterpart.

b) The assessment of the "risks to the rights and freedoms of data subjects" [Article 35(7)(c)].

These risks relate to possible future negative consequences of data processing operations, and more concretely, to harms brought about by such operations. Their assessment pertains to "physical, material or non-material damage" and includes e.g. discrimination, identity theft or fraud, financial loss or damage to reputation, loss of confidentiality, unauthorised reversal of pseudonymisation, any other significant economic or social disadvantage, loss of control over our own personal data, processing of unauthorised sensitive data or data from vulnerable natural persons, in particular children (Recital 75 provides a longer list of examples of such harms; further identification of risks occurs during the assessment process). The decision on whether a processing operation involves a 'risk' – and then – a 'high risk' pertains to a data controller and is done "on the basis of objective assessment" (Recital 76).

These risks pertain to natural people, including data subjects, and not to data controllers or processors. They concern the enjoyment of rights and freedoms by natural people; they are not compliance risks. Given the goal of the Regulation, these risks have a much wider scope than solely the right to personal data protection, extending to other rights and freedoms in an open-ended way (Recital 4 indicates rights such as privacy, effective remedy, fair trial, cultural, religious and linguistic diversity and freedoms such as freedom of thought, conscience and religion, freedom of expression and information or freedom to conduct a business).

Risks to the rights and freedoms are largely appraised qualitatively, by evaluating their severity (magnitude of a risk) and likelihood (feasibility of occurrence, e.g. low, medium or high), measured by a reference to "origin", "particularity" (Recital 84) and "nature, scope, context and purposes of processing" (Recitals 75-76). Certain data protection risks, e.g. data security risks, could be appraised quantitatively (e.g. their probability).

Under Art. 27(1) LED and Art. 89(1) EUDPR, risk appraisal is required.

The two appraisal techniques mentioned above are particularly relevant also for eIA. However, if any of the ethical concerns identified in the scoping phase is not touched upon by neither risk appraisal nor necessity and proportionality test, it is necessary to resort to other techniques to evaluate ethical impacts. These might regard, in particular, techniques to apply moral theories to further clarify the values at stake or to identify conflict of values (also in other fields) and propose ways to overcoming them.

2.3 Phase III: Recommendations

The recommendations phase can have a broader or narrower scope depending on the pillar of impact assessment that has been carried out. In case a DPIA is required, the assessment process shall be concluded with a list of recommended measures envisaged to: a) address the risks, "including safeguards, security measures and mechanisms to ensure the protection of personal data", and b) demonstrate compliance with the Regulation, "taking into account the rights and legitimate interests of data subjects and other persons concerned" [Art. 35(7)(d) GDPR and Art. 39(7)(d) EUDPR].

Similarly, under Art. 27(2) LED and Art. 89(2) EUDPR, the assessment shall contain at least a) the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and b) demonstrate compliance with the Directive/data protection rules, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

For what concerns privacy and ethics, it might be the case that the recommendations requested by the GDPR do not cover all the ethical and societal impacts of the initiative. If this is the case, the assessor could formulate recommendations on a broader scale (depending on the expertise of the team):

- Technical recommendations, including design interventions (e.g. to safeguard privacy, access control mechanisms, authentication mechanisms and encryption methods may be useful).
- Societal recommendations, including addressing issues of public trust and public concerns. It might be advised, for instance, to promote campaigns to help travellers familiarize to use the newest borderless crossing technologies.
- Organizational recommendations, such as suggesting drafting Internal (ethics) codes of conduct.
- Regulatory recommendations, in case the legal and ethical requirements are not met by the given initiative.
- Policy recommendations, e g. in the form of white papers addressed to decision-making authorities.

2.4 Phase IV: Ongoing phase

2.4.1 Stakeholder involvement (public participation) in decision-making:

The involvement of stakeholders is a key phase for the integration of the different pillars of the IIA. In fact, while with other phases/steps team members might work somehow independently (e.g. the scoping of potential impacts by narrowing down the benchmark), the stakeholders involvement exercise should be conducted once for all pillars. For instance, when stakeholders from different areas are consulted or reunited to discuss together, it is easier to identify potential conflicts of requirements (e.g. technical requirements vs privacy).

This phase follows, ideally, the phase of scoping, where stakeholders are initially identified and categorised, and runs throughout the whole process.

There are many challenges regarding stakeholders' involvement in an IIA. First, involving each category that has been identified may be challenging, especially when a category is very broad or vague (e.g. LEAs) or in a situation of particular vulnerability (e.g. irregular migrants). That is why the stakeholder involvement in decision making may be performed via e.g. NGO or other forms associations that

represent categories of stakeholders. Second, performing consultation for each phase of the assessment process is highly dependent on the scale and resources of the IIA, and might be difficult in cases there are not resources to do so. However, it should be stressed that this phase is of crucial importance and should not be neglected.

When a DPIA is required by law, stakeholder's consultation is also part of the process. Stakeholder consultation is foreseen in Art. 35(9) GDPR and 39(9) EUDPR, where appropriate and without prejudice for the protection of (commercial, in case of GDPR, or) public interests or the security of processing operations. The 'appropriateness' of consultation is not understood as 'optional'. Exceptions can be made if no new insight could be gained by their involvement or it would imply a disproportionate effort in relation to the results. A decision not to involve stakeholders, or to deviate from the results of such consultation, are reasoned and documented.

Albeit stakeholder consultation is not explicitly mentioned in Art. 27 LED and Art. 89 EUDPR, it should be performed. Moreover, in case of LED, national laws implementing the Directive may provide for stakeholder consultation.

Another stakeholder whose involvement is required under Art. 35(2) GDPR and Art. 39(2) EUDPR, but also recommended for DPIA in law enforcement, is the DPO.

As for ethics, stakeholder's consultation is particularly important when it comes to assessing the social acceptance of a given initiative among end users (e.g. through surveys or questionnaires, on spot or remotely). Discussing with stakeholders through focus groups, workshops and or citizens panels could help to merge the gap between social acceptance and more high-level ethical principles.

2.4.2 Documentation

The description of this step can be seen at Section 1.3 on the generic method.

In case of DPIA, albeit a written documentation is not required by law, is still advisable providing that data controllers must be able to demonstrate compliance.

2.4.3 Quality control

The description of this step is the same as the one provided in Section 1.3.

2.5 Phase V: Revisiting

In this step a decision is made as to whether to reconduct the assessment process entirely or in part. It can occur every time the envisaged initiative is modified (before or after its deployment) or the context in which it is going to be deployed, or already has been deployed, changes. This step ensures the continuity of the assessment process, e.g. in case of a transfer of the initiative to another organisation.

In case of a DPIA, when "necessary", "the controller shall carry out a review to assess if processing is performed in accordance with the [DPIA] at least when there is a change of the risk represented by processing operations" [Art. 35(11) GDPR and Art. 39(11) EUDPR]. This review can therefore occur merely after a period of time for monitoring purposes or when there is a change that rendered the previous assessment process obsolete (partially or totally). However, the Regulation does not stipulate

the consequences of such a review, yet – given a possible change of risk – the assessment process might need to be conducted again (in part or in total).

In case of DPIA in LED and for DPIA carried out by Union bodies, offices and agencies when carrying out activities which fall within the scope of Chapter 4 (Judicial cooperation in criminal matters) or Chapter (Police cooperation in criminal matters) 5 of Title V (Area of Freedom, Security and Justice) of part three TFEU data, there are no explicit provisions about revisiting of the DPIA, although, in case of LED, the revisiting may be foreseen in national laws implementing the Directive. We recommend nevertheless to perform the revisiting also for these processing operations.

Also, a PIA is a living instrument that should be revisited each time a project is changed and such a change impacts privacy.

3 Ready-made method for border control

This chapter will provide a ready-made method for borderless crossing technologies. Although the captions are the same as Chapter 2, Chapter 3 differs from the previous chapter as it indicates what to do step by step and it lists some techniques that could be used during the process. This ready-made version is still under development and will be updated in D3.2 in M24 of the project.

3.1 Phase I: Preparation of the assessment process

3.1.1 Screening (threshold analysis)

First of all, it is necessary to understand if EU law is applicable or if the matter falls entirely within national security.

If the latter, the data protection law related issues are regulated at national level.

If the former, then the data controller has to identify the right legal framework applicable, which could be: GDPR, LED -for which it will still be necessary to refer to national rules implementing the Directive, or EUDPR.

a) Under the GDPR and Art. 39 EUDPR, in order to determine whether a process of DPIA is required by law, the envisaged initiative has to be examined against the following six criteria:

i. *Criterion 1 – high risk*: at a most general level, the GDPR requires a process of DPIA to be carried out for processing operations likely to present high risk to the rights and freedoms of data subjects, taking into account four qualitative criteria of the nature, scope, context and purposes of the processing of personal data; and for data processing operations involving new technologies which constitute a particular trigger for the assessment process [Art. 35(1)]. These criteria, however, are not further defined, but could include e.g. the processing of special categories of personal data or data relating to criminal convictions and offences, data related to security measures or biometric data (i.e. the nature of processing operations), the amount of data processed, the geographical reach and the number of people affected (i.e. scope), in publicly accessible areas (i.e. context), data for profiling or automated decision-making (i.e. purpose) [cf. Recital 91]. It is for the data controller to determine whether a risk is "high", for which determination the controller is held accountable. High risk is the first criterion also for Art. 39 EUDPR.

ii. *Criterion 2 – enumeration*: the GDPR and Art. 39 EUDPR foresee three types of data processing operations for which a DPIA is required due to their likeliness to present high risk to the rights and freedoms of data subjects. These are:

- "systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person";
- processing, on a large scale, of special categories of data or of personal data relating to criminal convictions and offences;
- "systematic monitoring of a publicly accessible area on a large scale" [Art. 35(3)].

iii. *Criterion 3 – positive enumeration by data protection authorities*: a national or regional data protection authority (DPA) is entitled to determine, for its own jurisdiction, further types of data processing operations for which a process of DPIA is required [Article 35(4)].

In case of EUDPR, the European Data Protection Supervisor shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment.

iv. *Criterion 4 – negative enumeration by DPAs*: the same authority may determine, for its own jurisdiction, other types of data processing operations for which a process of DPIA is *not* required [Article 35(5)]. Both lists, if they involve – generally speaking – cross-border processing operations, are to be communicated to the European Data Protection Board (EDPB) for an opinion, for which the consistency mechanism applies [Article 35(4)-(6)].

In case of EUDPR, the European Data Protection Supervisor may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required.

v. *Criterion 5 – selected previous assessment processes*: unless Member States decide otherwise, for personal data processed in order to comply with a legal obligation [Article 6(1)(c)] or processed in a public interest [Article 6(1)(e)], on the basis of EU law or Member States law, which have been already assessed within an assessment process in the context of the adoption of that legal basis, the process of DPIA is no longer required, provided this other assessment process essentially satisfied conditions laid down in the GDPR [Article 35(10)].

In case of EUDPR, where processing pursuant to point (a) [processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body] or (b) [processing is necessary for compliance with a legal obligation to which the controller is subject] of Article 5(1) has a legal basis in a legal act adopted on the basis of the Treaties, which regulates the specific processing operation or set of operations in question, and where a data protection impact assessment has already been carried out as part of a general impact assessment preceding the adoption of that legal act, the process of DPIA shall not apply unless that legal act provides otherwise.

vi. *Criterion 6 – exemptions for specific professions:* in case the processing operation concerns "personal data from patients or clients by an individual physician, other health care professional or lawyer", these operations are not considered to be on a large scale and hence the process of DPIA is not required [Recital 91].

Such exemptions are not foreseen in the EUDPR.

If any of the first three criteria is satisfied, a process of DPIA is mandatory. Conversely, if any of the three last criteria (criteria 4 and 5 in case EUDPR) are satisfied, a data controller is exempted from carrying out the assessment process.

b) If a DPIA is mandatory, then also an eIA is required. If not, a threshold analysis questionnaire should be compiled. To determine the threshold of eIA, an example of ethics threshold analysis questionnaire is provided in the following table:[18]

[18] Adapted from (Brey, 2017), SATORI standard in CEN Workshop Agreement CWA 17145-2 ftp://ftp.cencenelec.eu/EN/ResearchInnovation/CWA/CWA17214502.pdf

Table 2: Ethics threshold analysis questionnaire

Please provide an answer between 1 (not severe) and 4 (very severe) to the following questions.		
Does the initiative could result in the development and/or use of technologies that:	**Score (1 to 4)**	**Comments**
1. Would not require/respect informed consent of the travellers?		
2. Would infringe freedoms of travellers?		
3. Would have a negative impact on users' identity?		
4. Could be misused (e.g. for terrorist purposes)?		
5. Would not accurately or reliably identify people?		
6. Would impact upon travellers' privacy?		
7. Would raise concerns of equality?		
8. Would not be accessible for certain categories of people?		
9. Would not have mechanisms for determining accountability (of the designers, customs, border police) in place?		
10. would not be transparent to its users?		
11. would not be compliant with legal requirements (or it is not yet clear if it does so)?		

If the score of any of the previous questions is >1, an eIA is warranted. If no threshold is met (i.e. no potential ethical issues are raised), an independent body (e.g. data protection authority for what concerns a DPIA, internal ethics committees or external advisory boards for ethics) should review the assessment form to ensure that this is the case.

c) If the answer to question 6 above is >2, a PIA is warranted.

In sum, the following decision tree will guide the assessor through the threshold analysis.

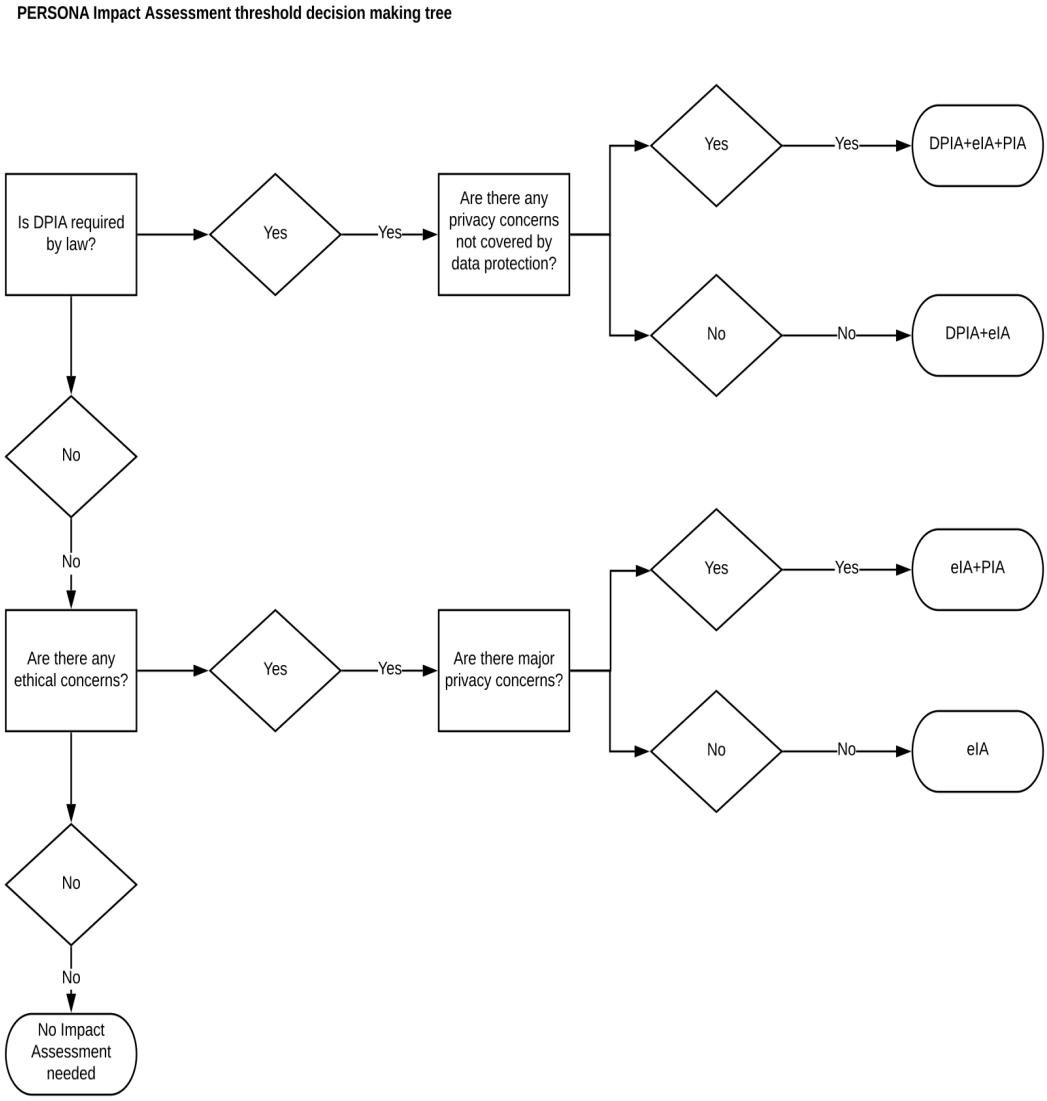

Figure 2: Decision tree guiding the threshold analysis

3.1.2 Scoping

The steps of the ethical scoping, integrated with the privacy and data protection scoping, are to preliminary identify:

a) The level of granularity of the initiative, and

b) Potential data protection, rights and freedoms of natural persons, privacy and ethical concerns on the topic or similar projects/technologies (if there are resources to do so). Please keep in mind that hiring external ethics experts or establishing an ethics advisory board might be necessary to complete this step.

The following techniques to identify potential ethical issues might be used (ideally all the four should be conducted in parallel, some of them could be omitted depending on the scale of the assessment):

- Literature review
- Checklist approaches
- Foresight methods
- Stakeholders consultation (ordered according to an increasing level of complexity): surveys, focus groups, roundtables, Delphi method, scenario methods

c) Categories of stakeholders who might affect or be affected by the project, such as:

- Law Enforcement Authorities
  - Border control authorities
  - Custom officers
- Policy makers (including legislators and executive, EU bodies and agencies)
- Travellers (which could be further distinguished in business travellers, families, minors, disabled people, elderly etc.)
- Irregular migrants (to be distinguished between asylum seekers and economic migrants)
- NGOs and human rights advocates
- Technology providers (e.g. biometrics, body scanners producers and other security solutions)
- Security service providers
- DPO
- Experts including academia
- Public opinion

d) Preliminary Identification for techniques of appraisal of impacts (see section 3.2.2)

e) Preliminary Identification for techniques for stakeholder involvement (see Section 3.4.1)

3.1.3 Planning and preparation

The planning phase is common to all the pillars of the IIA. This phase includes, among other things:

a) Determining the scale of the IIA (small, medium, large)
b) Estimating the budget
c) Estimating the timespan or duration of the process
d) Creating the team.

3.2 Phase II: Assessment

3.2.1 Description

1. Contextual description (Systematic description of envisaged processing operations and the purpose of the processing under GDPR and Art. 39 EUDPR, a general description of envisaged processing operations under LED and Art. 39 EUDPR)
2. Technical description of processing operations
3. “Big picture” description

3.2.2 Appraisal of impacts

DPIA under Art. 35(7) GDPR and under Art. 39(7) EUDPR provide for two types of appraisal techniques:

- necessity and proportionality test, and
- risk appraisal.

Under Art. 27(1) LED and Art. 89(1) EUDPR, it is risk appraisal.

As for ethics IA, suggested appraisal techniques are:

- Applied Ethics
- Ethical Checklist approaches
- Participatory methods
- Stakeholders consultation
- Scenario-based approaches

As regards privacy impact assessment, ISO standard ISO/IEC 29134:2017 *Information technology — Security techniques — Guidelines for privacy impact assessment*,[19] provides for risk assessment as appraisal technique. Other appraisal techniques include e.g. scenario planning and cost benefit analysis.

3.3 Phase III: Recommendations

For a DPIA:

a) the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and

b) the demonstration of compliance with the Directive/data protection rules, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

For an eIA and/or PIA:

- Technical recommendations, including design interventions
- Societal recommendations
- Organisational recommendations
- Regulatory recommendations
- Policy recommendations

3.4 Phase IV: On-going phase

3.4.1 Stakeholder involvement (public participation) in decision-making.

1. The first step in stakeholder involvement is their identification. Criteria to identify and categorize stakeholders:

[19] https://www.iso.org/standard/62289.html

- Internal vs external: the former group includes individuals and entities that are actively involved in the initiative at stake. The second group includes individuals or parties that are not as actively involved, but might be affected by its activities, and still play an important role in them.
- Primary stakeholders: high stake but low influence
- Key stakeholders: strong power position and major influence

2. The second step in stakeholder involvement is to define their level of involvement; Arnstein's typology of citizens participation, a continuum from low to high level of participation could be used as a general guidance.[20]

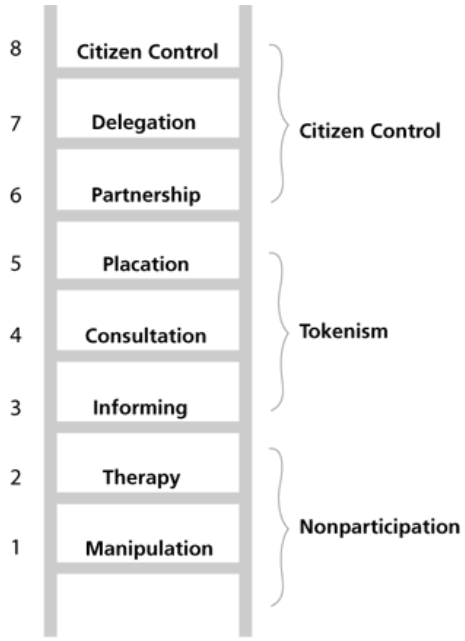

Figure 3: Arnstein's typology of citizens participation

Considering the requirements of a DPIA, and the history of the practices of IA (e.g. EIA, PIA), a 'high level' of engagement needs to be achieved here.

3. The third step is to involve stakeholders in the assessment process and there exists a plethora of techniques for doing so, namely:
   - *Focus groups*: small groups of people invited to discuss a theme and provide insights e.g. on values, concerns and perspectives involved in the given initiative.
   - *Roundtables*: participants agree on a specific topic to discuss. Each person is given *equal* opportunity to express her view, e.g. by allocating the same time slot for each participant to make comments on the initiative under discussion.
   - *(Scenario) Workshops*: a local meeting where small groups of key stakeholders gather to

[20] (Arnstein, 1969)

express a wide range of viewpoints and confront with each other. The discussion may also be triggered through the use of scenarios.

- *Interviews, questionnaires or surveys*: participants are asked specific questions on a given initiative, in a more or less structured way. The inputs gathered from the answers thereto are used to identify gaps, problems or potential solutions to a given initiative.
- *Delphi process*: people with different background take part in a series of facilitated discussions (without requiring face to face meetings, either by electronic or traditional correspondence). The input of the participants is anonymous.
- *Citizens panels*: citizens are recruited (e.g. by lottery) to serve their community by developing a range of options and deliberate upon one to address a given initiative.
- *Consultation with DPO* (when appointed).

3.4.2 Documentation

The outcome of the IIA process should be documented. It is advisable that the report follows, roughly, the structure and captions of the generic method. In any case, it should contain the following elements:

- Introduction
- Description of the initiative
- Description of the appraisal of the impacts
- Report of stakeholder's consultations
- Recommendations
- Summary of the outcomes.

3.4.3 Quality control

It might be advisable to ask for an independent evaluation of the IIA process. This for example could be carried out by external experts or by an external advisory board set up for this task. Such independent evaluation could:

- Provide constructive feedback and comments to improve the IIA
- Agree or disagree on the outcome of the IIA

3.5 Phase V: Revisiting

A review of the IIA process should take place several times throughout the whole process to ensure its components are up to date.

Ideally, a review should take place at least:

- At the start of the IIA
- During the IIA
- At the end of the IIA.

4 Operationalisation of the method

This chapter will provide two elements to help the assessor in the assessment process:

1) A checklist to guide the assessor through the steps enumerated in the last chapter.
2) A table with milestones for each step of the process

4.1 Checklist

The following table provides the assessor with a numbered list of questions grouped per step, from 'screening' to 'revisiting'. If the question regards a particular pillar or aspect of the IIA (e.g. DPIA or eIA) it is highlighted with a colour; if it is generic, it will have no colours. In particular:

- Questions regarding data protection are in red;
- Questions regarding ethics in purple;
- Questions regarding privacy in blue;
- Questions regarding social acceptance in orange.

Step	Number	Question
1. Screening	1	Does the matter fall within European law or is purely national security, meaning that national law will be applicable?
	2	Who is processing personal data and for which policy area (e.g. law enforcement or border management)?
	3	Does the no-gate crossing point solution represent a new technology or a new combination of existing technologies?
	4	Are the 6 criteria of GDPR satisfied?
	5	Are the 5 criteria of Art. 39 EUDPR satisfied?
	6	In conclusion, is a DPIA required under EU law, national law or a code of conduct?
	7	If a DPIA is not required, is an eIA required? (See threshold analysis questionnaire section 3.1.1)
	8	If an eIA is required, do the main ethical impacts concern privacy?
2. Scoping		a. Identification of the scale of the initiative
	9	What is the level of granularity of the given initiative? (E.g. a single device or an assemblage of technologies)
	10	Where will the initiative be implemented?
		b. Identification of potential concerns

	11	Does the no-gate crossing point solution fall within the dual use items regulation?
	12	Does the no-gate crossing point solution comply with UAVs related rules ?
	13	Whereas the no-gate crossing point solution is processing biometric data to be checked against an EU database, does the biometric data processed comply with technical requirements provided for in the database-related implementing rules?
	14	In case of EU large scale database, do only competent authorities access only those data, as provided for in the law, in the performance of their tasks? Who are the (joint) data controllers? And who are the data processors?
	15	Is the no-gate crossing point solution applied only at an external border or at an internal border temporarily reintroduced/not yet lifted?
	16	Is the no-gate crossing point solution physically located in an area where the border check is allowed (e.g. for airports NORMALLY not on the plane nor at the gate)?
	17	Has the no gate crossing point solution enabling automated border control system been designed in such a way that it can be used by all persons, with the exception of children under 12 years of age?
	18	Is there a sufficient number of staff to assist persons with the use of such systems available?
	19	Has the no-gate crossing point solution been designed in a way to support border guards in their duty to respect human dignity in the fulfilment of their tasks?
	20	Is the informed consent of travellers respected?
	21	Does the initiative infringe freedoms of travellers?
	22	Does the initiative have a negative impact on users' identities?
	23	Could the technologies be misused?
	24	Could the technologies unreliably identify people?
	25	Could the technology raise concerns of equality?
	26	Could the initiative be inaccessible for certain categories of people?
	27	Does the technology impact upon travellers' privacy?
	28	How do users perceive the facilitating features of the initiative? Is it 'easy to use?

	29	How do users perceive the security of the initiative?
	30	Is there a 'social pressure' to use the technology?
	31	Do the users trust the technology?
		c. Identification of categories of stakeholders
	32	Who are the stakeholders that might affect, be affected, concerned or interested in the initiative?
	33	How can such stakeholders be categorized?
		d. Identification of techniques for appraisal of impacts
	34	Which necessity and proportionality test could be used?
	35	Which risk appraisal standard could be used?
	36	Which ethics appraisal technique could be used?
		e. Identification of techniques for stakeholder's engagement
	37	Which techniques for stakeholder's engagement could be used?
3. Planning	38	What is the scale of the impact assessment? (Small/medium/large)
	39	What is the budget of the IA?
	40	What is the expected duration of the process?
	41	What members of the IA team are needed?
4. Description	42	Has a systematic (or general in case of DPIA under LED and Art. 89 EUDPR) description of processing operations been provided?
	43	Is there a technical description of data flows?
	44	Which personal data is the no-gate crossing point solution processing?
	45	Is the no-gate crossing point solution collecting biometric data other than fingerprints and facial images?
	46	Have the data subjects been informed?
	47	What is the legal basis for the data processing?
	48	Are data collected for specified, explicit and legitimate purposes and no further processed in a manner incompatible with those purposes?
	49	Are the data collected adequate, relevant and limited to what it is necessary in relation to the purposes for which they are processed?
	50	Are data accurate and kept up-to-date?

	51	Are data kept for no longer than necessary for the purposes for which they were collected?
	52	Do data subjects have the right to access, directly or indirectly, their data?
	53	Do data subjects have the right to rectify inaccurate data?
	54	Do data subjects have the right to erase unlawfully stored data?
	55	Is human intervention foreseen in case of automated decision making?
	56	Are third parties involved in the processing of personal data?
	57	Do data subjects have the right to lodge a complaint or seek for a judicial remedy in case their rights have been violated?
	58	Are there procedures into place if biometrics data become unreadable (e.g. unreadable fingerprints, people with only one hand or older people)?
	59	Are the technologies accessible for people with reduced mobility (e.g. on a wheelchair)?
	60	Are there mechanisms to ensure the accountability of borderless crossing technologies designers?
	61	Are there mechanisms to ensure the accountability of borderless crossing technologies customs?
	62	To what extent is it possible to keep track of the system's data? Are there mechanisms in place to ensure the traceability of the system's processes and outcomes?
	63	To what extent the outcomes of the system can be explained?
	64	To what extent the system's decision influence the border guard/custom?
	65	If you are using an AI system, did you communicate the users they are not interacting with a human?
	66	Did you communicate about potential risks or bias?
	67	Is the technology compliant with current regulatory requirements?
	68	To what extent is the technology transparent to its users?
	69	Is there a 'fallback plan' in case the system is not working properly?
	70	To what extent is the system resilient to attacks and security?

	71	How accurate is the system for identification?
	72	How reliable are matches made by the system?
	73	What are the security measures in place?
	74	Are there mechanisms to ensure human intervention in case of false positives or negatives?
5. Appraisal		a. Necessity & Proportionality
	75	Is the no-gate crossing point solution restricting fundamental rights (e.g. privacy, data protection, asylum …)?
	76	What are the purposes for which the no-gate crossing point solution has been implemented?
	77	Is the no-gate crossing point solutions necessary to achieve the goal foreseen?
	78	Is the no-gate crossing point solution proportionate in the light of the goal to achieve?
		b. Risk appraisal
	79	What are the possible risks of the given initiative?
	80	Does the no-gate crossing point solution entail processing operations likely to result in a high risk to rights and freedoms of natural persons?
		a. Ethics impacts appraisal
	81	To what extent is freedom of movement of travellers (especially vulnerable ones) infringed?
	82	To what extent is freedom of association of travellers (especially vulnerable ones) infringed?
	83	Will the technology be widely available or just for privileged groups (e.g. bona fide travellers)?
	84	Will the benefits/potential risks be equally distributed among the users?
	85	If there are possibilities to opt-out/resist, are such possibility equally accessible? Or is there an information asymmetry?
	86	Will the technology increase the 'digital divide'?
	87	Is the technology accessible to 'digital immigrants' (as opposed to 'digital natives')?
	88	Did any bias ever occur before in similar cases? Is it possible to prevent it?
	89	Is there a risk of over confidence or reliance?
	90	Is there any risk of physical or psychological harm to travellers?

	91	Can certain medical conditions of users be identified from the processing of biometric data?
	92	Are there any health and hygienic concerns about the use of biometrics?
	93	Is bodily integrity of travellers threatened?
	94	How does the presence of surveillance means govern our behaviour and affect our choices?
	95	How does the technology interfere with one's identity?
	96	Does the technology contradict people's narrative identity?
	97	Does the traveller have control over how she is represented to others? To what extent?
	98	Does the system seek to reveal individual's thoughts, beliefs or religious identities?
	99	Does the system impact upon bodily privacy?
	100	Does the system involve searching a person's body?
	101	Does the system involve taking bodily tokens (e.g. retina scans) without consent?
	102	Does the system require to provide biometric data?
	103	Can biometric data required by the system provide additional sensitive information (e.g. ethnic background or medical conditions)?
	104	Does the system impact upon behavioural privacy?
	105	Does the system involve monitoring a person's behaviour?
	106	Does the system involve tracking one's gait?
	107	Does the system involve recording one's voice?
	108	Does the system impact upon communicational privacy?
	109	Does the system involve access to someone's email or other communications (e.g. through the use of an app)?
	110	Does the system impact upon associational privacy?
	111	Does the system involve tracking of groups of individuals?
	112	Do group characteristics (e.g. gender, skin colour) play a role in determining whether tracking takes place?
	113	Can the categories resulting from group characteristics be considered discriminatory?
	114	Are the groups and the ways people are categorised made transparent and available to individuals?

	115	Do people have control over personal information when using the system?
	116	Do people have the necessary resources to use the system?
	117	Do people have necessary knowledge (e.g. information, data literacy) to use the system?
	118	Is guidance available to 'new' users?
	119	Are specialised instructions available for certain categories of people (e.g. disabled people or with reduced mobility)?
	120	Is a specific person available for assistance in case it is needed?
	121	Does a no-gate crossing system feel more secure than a traditional one?
	122	Are the security measures perceived as being disrespectful?
	123	Are the security measures perceived as being discriminatory?
	124	Are the security measures perceived to be disproportionate impact on travelling experience?
	125	Do influent/important people think users should use the system?
	126	To what extent airports and other border crossing points support the use of the system?
	127	To what extent airports and other border crossing points help using the system?
	128	To what extent airports and other border crossing points force users using the system?
	129	Do people who use the system have more prestige/visibility than people who do not?
	130	Do people know how their personal data will be managed?
	131	Do people trust the authorities managing their personal data?
	132	Do people trust the biometrics systems correctly identifying them?
6. Recommendations	133	Does the assessment contain recommended measures envisaged to address the risks, "including safeguards, security measures and mechanisms to ensure the protection of personal data"?
	134	Does the assessment demonstrate compliance with applicable data protection rules?

	135	Are controllers and processors implementing data security measures (psudonymisation and encryption, ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services…)?
	136	What technical recommendations could be given, if any?
	137	What societal recommendations could be given, if any?
	138	What organisational recommendations could be given, if any?
	139	What regulatory recommendations could be given, if any?
	140	What policy recommendations could be given, if any?
7. Stakeholder's involvement	141	What is the level of involvement of stakeholders?
	142	What stakeholders techniques could be used, given the scale of the assessment?
	143	At which phases of the process should the stakeholders involvement be conducted?
8. Documentation	144	Is the data controller capable to demonstrate compliance?
9. Quality Control	145	Is an independent evaluation for the process needed? If yes, who should carry it out?
	146	Are3 there any feedback/comments on the output of the quality control?
10. Revisiting	147	Did a review take place during the process?
	148	Did a review take place at the end of the process?

4.2 Milestones

The following table provides a list of 28 milestones, divided into phases (from 'screening' to 'revisiting'), along with a short description.

	Milestones	Description
Phase I		
1) Screening (if threshold is not met, go to M24)	M1	Determination of whether DPIA is required by law
	M2	Determination of whether the threshold for eIA/PIA is met
2) Scoping	M3	Identification of data protection concerns
	M4	Identification of risk to rights and fundamental freedoms concerns
	M5	Identification of privacy concerns

	M6	Identification of ethical concerns
	M7	Identification of categories of stakeholders
	M9	Identification of appraisal techniques
	M10	Identification techniques to involve stakeholders
3) Planning	M11	Determination of the scale of the assessment
	M12	Estimation of the budget
	M13	Creation of team of assessors
	M14	Consultation of DPO (if required)
Phase II		
4) Description	M15	Compilation of a "broad picture" description of the initiative
	M16	Compilation of a contextual description of processing operations
	M17	Compilation of a technical description of processing operations
5) Appraisal of impacts	M18	Risk assessment techniques carried out (for DPIA)
	M19	Necessity and proportionality test carried out (for DPIA)
	M20	Appraisal techniques for eIA/PIA carried out (if necessary)
Phase III		
6) Recommendations	M21	Creation of a list of measures to address the data protection risks and demonstrate compliance with legal statutes
	M21	Creation of a list of measures to address ethical/privacy risks
Phase IV (on-going)		
7) Stakeholder involvement	M23	Performance of stakeholders involvement (see M7, M8, M9)
8) Documentation	M24	Issuance of the report/statement of non-significant impact (if it is the case)
	M25	Compilation of IIA final report
9) Quality control	M26	Independent evaluation took place
Phase V		
10) Revisiting	M27	Plan a periodical review of the process
	M28	Periodical review carried out

5 Concluding remarks

Deliverable D3.1 presented an initial version of the PERSONA impact assessment method. Chapter 1 contained an overview of the impact assessment vocabulary. Chapter 2 and 3 focused on the impact assessment method, first from a more theoretical perspective, and secondly from a more practical standpoint. Finally, Chapter 4 included an operationalisation of the method, providing a checklist and a list of milestones to guide the assessor through the process.

The method provided in this deliverable is an initial version and will be updated in M24, taking into account the results of the test studies as well as the feedback received by the EAB and CoS. The work carried out in this deliverable will be one of the main sources of the PERSONA textbook (D5.2/D5.3, first and final version respectively).

6 Bibliography

Arnstein, S. R. (1969). A Ladder Of Citizen Participation. *Journal of the American Institute of Planners*, *35*(4), 216–224. https://doi.org/10.1080/01944366908977225

Brey, P. (2017). Ethics of Emerging Technology. *The Ethics of Technology Methods and Approaches*.

City of Westminster. (2019). *City Plan 2019-2040 - Integrated Impact Assessment report*.

Kloza, D., van Dijk, N., Casiraghi, S., Vazquez Maymir, S., Roda, S., Tanas, A., & Konstantinou, I. (2019). Data protection impact assessments in the European Union: designing an appraisal method towards a more robust protection of individuals (forthcoming). *D.Pia.Lab Policy Brief, VUB*, *2*, 4.

Kloza, D., van Dijk, N., Gellert, R., Böröcz, I., Tanas, A., Mantovani, E., & Quinn, P. (2017). 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, VUB: Brussels*, *1*.

Koops, B. J., Newell, B. C., Timan, T., Škorvánek, I., Chokrevski, T., & Galič, M. (2017). A typology of privacy. In *University of Pennsylvania Journal of International Law* (Vol. 38).

London Plan. (2017). *GLA London Plan IIA*. (November). Retrieved from www.arup.com

Smismans, S., & Minto, R. (2017). Are integrated impact assessments the way forward for mainstreaming in the European Union? *Regulation & Governance*, *11*(3), 231–251. https://doi.org/10.1111/rego.12119

Tajima, R., & Fischer, T. B. (2013). Should different impact assessment instruments be integrated? Evidence from English spatial planning. *Environmental Impact Assessment Review*, *41*, 29–37. https://doi.org/10.1016/j.eiar.2013.02.001

Valkenburg, G., & van der Ploeg, I. (2015). Materialities between security and privacy: A constructivist account of airport security scanners. *Security Dialogue*, *46*(4), 326–344. https://doi.org/10.1177/0967010615577855

Vanclay, F. (2004). The triple bottom line and impact assessment: How do TBL, EIA, SIA, SEA and EMS relate to each other? *Journal of Environmental Assessment Policy and Management*, *6*(3), 265–288. https://doi.org/10.1142/9789814289696_0006

Wright, D., & De Hert, P. (2012). Privacy impact assessment. In *Privacy Impact Assessment*. https://doi.org/10.1007/978-94-007-2543-0