8 A tailored method for the process of integrated impact assessment on border control technologies in the European Union and the Schengen Area

Nikolaos Ioannidis,* Simone Casiraghi,** Alessandra Calvi*** and Dariusz Kloza****

* *Vrije Universiteit Brussel. E-mail: Nikolaos.Ioannidis@vub.be.*

** *Vrije Universiteit Brussel. E-mail: Simone.Casiraghi@vub.be.*

*** *Vrije Universiteit Brussel. E-mail: Alessandra.Calvi@vub.be.*

**** *Vrije Universiteit Brussel. E-mail: Dariusz.Kloza@vub.be.*

Introduction

The purpose of this Chapter is to provide sufficiently detailed explanations to enable the completion of the Template for reporting the integrated impact assessment process (Annex 1). The assessors consult this Chapter's instructions in conjunction with Annex 1, whose structure firmly corresponds to the structure herein.

The Template for reporting the integrated impact assessment process in Annex 1 is organised into tables and matrices. Following the 11-step method, consecutive steps are marked in brown and the ongoing steps in orange, as presented in the diagram below. The assessors are to fill in only the fields coloured in light brown or light orange. A field for any further remarks or comments, if necessary, is provided at the end of each step. The

DOI: 10.46944/9789461171375.8

assessors fill in, in an easily understandable language, the empty rows in the tables and/or other fields assigned to each step. To the greatest extent possible, each answer is exhaustive and sufficiently motivated (described, explained, justified, etc.), as is equally the case for the criteria/explanations 'fulfilled' and 'not fulfilled'. Further rows can be added in each table, should there be a need, or, should the space be insufficient, each element can be moved to attachments. Alternatively, any of the tables and/or fields may be removed, and the same information presented in some other format if the assessors deem it appropriate. Provision of an explanation is required whether the box is ticket or not. After the receipt of the filled-in report, the sponsoring organisation, in turn, fills in the light green fields only, facilitating the final decision (of whether or not to proceed with the envisaged initiative).

The Template assumes the team of assessors is familiar with the legal framework for personal data protection and privacy in the European Union, as well as the principles of ethics and social acceptance. (References to legal provisions without any further specification pertain to the General Data Protection Regulation [GDPR].) It also assumes minimum familiarity with the process of risk appraisal and with the criteria limiting the enjoyment of human rights, in particular those of necessity and proportionality. Furthermore, it is expected that all relevant stakeholders, be they the data controller(s), the data protection officer (DPO), the pertinent EU agencies and border control authorities, among others, are involved in the entirety of the assessment process. As the assessment process concerns an as-yet-unimplemented initiative, the assessors may have to rely on estimations and, at times, incomplete information.

Overview of the method

Start

ONGOING PHASE

[A] Stakeholder involvement
Identify, define the level of involvement and involve stakeholders at different phases of the process

[B] Quality control
Check the quality of the IIA process (internally or externally)

[C] Documentation
Document the IIA process

Steps	Data Protection	Ethics	Social Acceptance	Privacy
PHASE I: PREPARATION OF THE ASSESSMENT PROCESS				
[1] Screening	**[1a]** Preliminary description			
	[1ba] Data protection screening	**[1bb]** Ethics and social acceptance screening		**[1bc]** Privacy screening
[2] Scoping	**[2aa]** Personal data protection benchmark	**[2ab]** Ethics benchmark	**[2ac]** Social acceptance benchmark	**[2ad]** Privacy benchmark
	[2b] Stakeholders and their consultation techniques			
	[2c] Appraisal techniques			
	[2d] Other evaluation techniques			
[3] Planning and preparation	Objectives ♦ criteria for acceptability of negative impacts ♦ resources ♦ procedures and timeframes of the assessment process ♦ assessors ♦ stakeholders ♦ continuity of the assessment process ♦ criteria triggering a revision			
PHASE II: ASSESSMENT				
[4] Systematic description of the initiative				
[5] Appraisal of impacts	**[5aa]** Data protection: Necessity and proportionality of the processing operations **[5ab]** Data protection: Risk to the rights and freedoms of natural persons	**[5b]** Ethics assessment	**[5c]** Social acceptance assessment	**[5d]** Privacy impact assessment
	[5e] Legal compliance check			
[6] Recommendations				
PHASE III: EX-POST (EVENTUAL) STEPS				
[7] Prior consultation with supervisory authority				
[8] Revisiting				

The end

PHASE I: PREPARATION OF THE ASSESSMENT PROCESS

Step 1: Screening (threshold analysis)

The goal of this Step is to determine if the impact assessment process is required in the first place. Conducting the impact assessment process is necessary when one or more criteria set forth by law (for data protection and privacy) or by other principles (ethics and social acceptance) are met, or, alternatively, it is not required when a pertinent exemption is provided. This is preceded by the preliminary description of the initiative, which provides a contextual and a technical overview thereof.

Step 1a: Preliminary description

In this part, the assessors briefly expose the most critical aspects of the envisaged initiative, answering questions about the context and technical aspects thereof. The overview is quadripartite, comprising the assessment benchmark, namely: i) the right to data protection; ii) the right to privacy; iii) ethics; and iv) social acceptance. Although little information is usually available at the early stages, the preliminary description is kept short (approx. one page), while still being sufficiently detailed to allow the assessors to determine whether or not the threshold criteria are satisfied. General statements are avoided. If, in Step 1b, it is determined that the assessment process is required, this preliminary description will be expanded in Step 4.

Step 1b: Screening

Step 1ba: *Data protection*: The assessors analyse whether the envisaged data processing operations satisfy any of the threshold criteria prescribed by law. As a prerequisite, the assessors determine if personal data would be processed within the envisaged initiative. The threshold criteria are based on the concept of risk, and are either positive or negative. The negative criteria take precedence over positive ones. If any of the positive criteria are satisfied, the assessment process for the right to personal data protection will then be required by law. By contrast, if any of the negative criteria are satisfied, the data controller is exempted from conducting such an assessment process.

Step 1bb: *Ethics and social acceptance*: The assessors determine whether the envisaged initiative raises any ethical or social acceptance challenges by answering a set of questions. If *any* of them is answered affirmatively, the ethics assessment and social acceptance assessment are required. Conversely, if *all* are answered negatively, there is no need for an ethics and social acceptance assessment. The assessors proceed to this Step in order to complement the data protection element (Step 1b), when this is required.

Step 1bc: *Privacy*: The assessors determine if the envisaged initiative interferes with any of the 9 dimensions of privacy, i.e. bodily, spatial, communicational, proprietary, intellectual, decisional, associational, behavioural and informational privacy. If *at least one* type

of privacy is interfered with, then a privacy impact assessment is required. Conversely, if *none* is interfered with, there is no need for a privacy impact assessment.

If no integrated impact assessment process is required or warranted, the assessors prepare a reasoned statement of no significant impact.

Step 2: Scoping

The goal of this Step is to identify, with a reasonable degree of precision:

- the benchmark of the integrated impact assessment, in which case, four elements are examined in particular: i) the right to data protection; ii) the right to privacy; iii) ethics; and iv) social acceptance (Step 2a)
- the categories of stakeholders, that is, those to involve in the assessment process and how to involve them in each Step (Step 2b)
- appraisal techniques, other than the necessity and proportionality assessment, and risk assessment, to be used in the assessment process (Step 2c)
- other evaluation techniques that may be warranted or necessary (Step 2d).

Step 2a: Benchmark

Step 2aa: *Data protection*: The assessors first map the aspects that the envisaged data processing operations would touch upon by checking the applicable laws and regulations. The assessors list all legal (national, European, international) and regulatory instruments applicable to the initiative, including by-laws (e.g. policies, codes of conducts, technical standards) applicable within the organisation. This also constitutes the legal and regulatory framework for border management, from which compliance requirements are inferred and checked against in Step 5.

Step 2ab: *Ethics*: The assessors identify the ethical arguments that are mobilised to support or criticise the initiative in the public debate. Each set of arguments is assigned an ID that will be used in the subsequent phases of the assessment. This task requires that the assessors perform some preliminary desk research (if necessary, they can ask external researchers to provide support in this regard). The assessors fill in the relevant table in the template by ticking the arguments that apply to the initiative, with the help of the examples provided and explained in Chapter 5. The assessors may add extra arguments through the addition of extra rows, as indicated in '1.x …', '2.x …' etc.

Step 2ac: *Social acceptance*: The assessors identify three aspects: the perspective to assess social acceptance, the categories of stakeholders and the acceptance assessment techniques. Regarding the perspective of social acceptance, the assessors choose between (at least) one of the three levels indicated in Chapter 6 (i.e. socio-political, community or market perspective) and tick the chosen level. An assessment of all three perspectives is not required, yet, the focus *must not* be exclusively on the market perspective. The assessors identify a list of stakeholders that is specific for the social acceptance assessment. Stakehol-

ders are understood in the broadest sense, and their range and the number to be involved is commensurate to the processing operations. Stakeholders are *not* assessors; the former provide input, which the latter subsequently take into account or reject. This activity can be performed in parallel with the identification of stakeholders for the 'stakeholder involvement phase' (Step 2b), which will provide the assessors with a broader list to be consulted throughout the whole impact assessment process. The sample chosen, especially for travellers, is to be as representative as possible. The assessors choose at least one technique of stakeholder involvement, without relying too heavily on questionnaires, especially if they are close-ended and require a quantitative analysis. Finally, the responses from the questionnaires can be made more robust by informing the respondents about the initiative under assessment with, for example, informational meetings or technology demonstrations.

Step 2ad: *Privacy*: The assessors identify which types of privacy will form part of the benchmark, and justify why these identified types are interfered with. To do so, they will briefly describe the interference, the circumstances and the vulnerability that is produced due to the contact of a natural person with a specific technology, using the same types of privacy that they included in the previous step. Additionally, they will determine the appraisal techniques that they deem most pertinent (usually the privacy impact assessment) and the stakeholders, who may be the same as those involved in the data processing operations.

Step 2b: Stakeholders and their consultation techniques

In this step, the assessors identify the categories of stakeholders to be consulted throughout the impact assessment process, namely internal and external stakeholders. The list is broader than the one compiled for Step 2a (social acceptance scoping). Possible techniques to involve stakeholders are provided in Annex 2 of this Volume. Critical external stakeholders in the context of border management law are EU agencies and bodies, carriers, Passenger Information Units (PIUs) and technology providers, among others.

Step 2c: Appraisal techniques

Six appraisal techniques are foreseen, corresponding to the quadripartite benchmark: (a) necessity and proportionality, and (b) risk assessment for data protection; ethics assessment for ethics; privacy impact assessment for privacy; social acceptance assessment for social acceptance; legal compliance check against data protection, privacy, ethics requirements, inferred from border management law as identified in Step 2a (the legal compliance check is expected to enhance social acceptance, too). Should these six appraisal techniques prove to render insufficient information for decision-making purposes, other appraisal techniques should be employed, as listed in Annex 3, e.g. scenario analysis (planning), technology foresight or cost–benefit analysis (CBA).

Step 2d: Other evaluation techniques

The assessors can resort to other evaluation techniques, which may be warranted or even required by law. For example, if the envisaged initiative *also* affects the natural and/or hu-

man environment, then a standalone process of environmental impact assessment (EIA) may be needed alongside the integrated impact assessment process.

In addition, for the reasons of comprehensiveness and efficiency, various types of impact assessment and other evaluation techniques can be integrated, provided the benchmark and/or appraisal techniques are coherent, not subordinate to one another, and not internally contradictory. Results of such an integrated assessment process must then be synthesised.

Step 3: Planning and Preparation

> The goal of this Step is to set the terms of reference of a given impact assessment process, constituting a written manual therefor, which may possibly be updated throughout the assessment process. For all parts of the benchmark, the assessors can devise a common approach since the resources and the timeframes of each separate assessment should align with each other.

Specific objectives of a given process: On the one hand, the substantive goal of an impact assessment process is to ensure informed decision-making by comprehensively examining the elements of the benchmark. On the other, its formal goal is to comply with the law and ethical or social norms. The impact assessment process aims to ensure both goals are achieved by aiding the decision-making process as to the deployment of the initiative; however, the assessors may clarify in greater detail the specific objectives of a given assessment process.

Acceptability criteria of negative impacts: The criteria are set and justified for each element of the benchmark and for each appraisal technique employed (cf. Step 2c). For instance, the element of data protection requires that the data controller set and justify a threshold below which a processing operation would be deemed unnecessary and/or disproportionate. Furthermore, it requires that the controller set a threshold above which a risk to a right would no longer be deemed acceptable (e.g. risk-prone, or risk-adverse). The data controller defines both the likelihood and severity scales beforehand. The same exercise can be repeated for each element of the benchmark, with respect to the nature and specificities of each. Jurisprudence in border control, relevant legislation and common practices are, among others, ideal sources for setting the acceptability criteria of negative impacts.

Resources to be committed: The assessors list and ensure the resources which they need for conducting the impact assessment process, which include time, money, workforce, knowledge, know-how, premises and infrastructure. Assessors might resort to the help of software that facilitates the impact assessment process by automating parts thereof. Lastly, the choices of locations (e.g. a venue for a workshop or for a facility tour) or setup (e.g. of a technology demonstration) further contribute to the selection of resources.

Procedures and timeframes: The assessors establish the timeframes for an impact assessment process, specifying, for example, milestones and deadlines, assigning responsibilities

and specifying who is answerable to whom within the organisational structure. For example, the ethics assessment is connected to the preparation of paperwork required in order to obtain the ethical approval and/or opinion from the relevant ethics committee or competent authority of the country hosting the study. The latter applies especially if (sensitive) personal data of people are processed during the assessment.

Team of assessors, and their roles and responsibilities: The assessment process requires multiple types of expertise. The organisation responsible for the initiative chooses the assessors on the basis of transparent criteria, either internal or external (outsourced), spelling out their roles and responsibilities, and ensures their professional independence (e.g. assessors do not seek nor receive instructions; their bias is explicitly marked as such).

Stakeholders: Based on the pre-defined categories in Step 2b, the assessors identify a list of stakeholders (e.g. a minimum number of people interviewed, number of participants in the workshop, etc.), taking into account and ensuring diversity (e.g. gender balance, geographic diversity, age diversity or multidisciplinarity). For large-scale consultations, a consultation plan may be necessary. Personal data of identified stakeholders is appropriately protected. The planning includes:

- dates and timespan of the assessment (e.g. duration of interviews);
- setup (e.g. of a technology demonstration);
- questionnaire or interview design;
- number and modality of stakeholders to involve (e.g. a minimum number of people interviewed, number of participants in the workshop, etc.).

Continuity: The organisation specifies the continuity of the assessment process in the event of, for example, changes in the actors involved in the assessment process (e.g. assessors, data controller, data processors, etc.), or disruption, natural disasters, or utility failures.

Revision: The organisation specifies the criteria that would trigger the revision of the impact assessment process. For instance, with regards to the data protection element, a change in the level of risk could be enough to trigger the revision of the whole process. The level of risk depends on the technological advancements, on the users' perception of a technology, or on a landmark court decision that re-interprets a legal provision. The decision as to whether to revise the entire process or just a part of it is dependent on the degree to which the elements of the benchmark are intertwined with each other.

PHASE II: ASSESSMENT

Step 4: Systematic (detailed) description of the initiative

The goal of this Step is, by expanding the preliminary description (cf. Step 1a), to systematically describe the envisaged initiative both contextually and technically.

A long list of factors is to be taken into consideration in relation to the right to data protection. As an illustration, contextual aspects include the nature, scope, internal and external context, and purposes of the envisaged processing operations and, when applicable, the legitimate interest pursued by the data controller. Technical aspects include diagrams of data flows and/or other visualisations, which might be appended. Such a description can also be based on the records of processing operations. Continuing the systematic description with regards to the right to privacy, the assessors identify, for example, the actors and parties involved in the initiative, the scope of the right based on the nine aforementioned types of privacy, and the level and nature of intrusiveness, among others. Lastly, a detailed description relevant to the ethics and social acceptance of the initiative may involve a description of the broader ethical and societal impact of the initiative, beyond those of the right to privacy and data protection.

The critical difference in the systematic description, compared to the preliminary one, is that it must expand the latter (cf. Step 1a), and hence needs to be much lengthier and more comprehensive. It shall be sufficiently complete, accurate and reliable so as to constitute the basis for the analysis and assessment of impacts in Step 5.

Step 5: Appraisal of Impacts

The goal of this Step is to analyse and assess the impacts of the envisaged initiative, appraised in accordance with the pre-selected techniques. These impacts pertain to the societal concern(s) that might be touched on by the planned initiative, and to the positioning of the stakeholders, who might be external to the sponsoring organisation. Typically, the assessment consists of a detailed identification, analysis, and evaluation of the impacts.

Step 5a: Data protection

Step 5aa: *Necessity and proportionality of the processing operations:* The assessors use specific appraisal techniques pre-defined in Step 2c and base their analysis on the results of Step 4. The assessors can use any of the numerous suitable methods made available thus far, or they can employ the one proposed in Annex 1. Contrary to methods for assessing

risk (e.g. international standards, such as ISO 31000:2018 or ISO 27005:2018), methods for assessing proportionality and necessity in the context of personal data protection are rather scarce.

The assessment of necessity and proportionality can occur at two levels. First, each data processing operation is assessed against personal data protection principles (Level 1). These are: lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and confidentiality, including security of processing and data protection by design and by default. Each data processing operation is assessed in a specific table, with this table needing to be replicated for each data processing operation.

Given the fact that a fundamental right is at stake and that an assessment process of the envisaged processing operations against solely personal data protection principles (Level 1) might not always be sufficiently complete, to the detriment of the level of protection and the quality of the decision-making process it is intended to advise, the assessors may decide to expand their appraisal to the entirety of human rights limitation criteria (Level 2).

As the right to personal data protection and many related fundamental rights are not absolute but rather relative ones (i.e. an interference with the right can only be justified under certain conditions), the following five limitation criteria derived from Article 52 of the CFR can be applied:

- legality (i.e. if a basis for a data processing operation is 'provided for by law' of a sufficient quality, for example, clarity, accessibility, precision, foreseeability, conformity with the rule of law);
- the respect for the essence of a right (i.e. if the interference with a fundamental right does not make it impossible to exercise a right);
- legitimacy (i.e. if a processing operation serves a given 'general interest' (cf. e.g. Article 3 Treaty on European Union (TEU)) or 'protect[s] the rights and freedoms of others');
- necessity (i.e. if a processing operation is 'necessary and [if it] genuinely meet[s]' legitimate objectives); and
- proportionality *sensu stricto* (e.g. balancing) (i.e. if the least intrusive option has been chosen).

Step 5ab: *Risk to the rights and freedoms of natural persons:* On the grounds of data protection law, risk is understood as a negative consequence arising from processing operations that might or might not occur in the future. Such a consequence, if it materialised, would give rise to physical, material or non-material damage for natural persons (largely, data subjects) and not solely for the data controllers or data processors. Risk assessment is meant to be as objective as possible; this is, however, not always achievable in practice, due to ambiguities about assignable likelihoods and possible types of damage, and the subjectivity of perceptions of risk by stakeholders.

Risk is typically assessed by combining two measurements, namely its likelihood or probability (i.e. chance of happening) and its severity (i.e. magnitude of consequences).

Risk can be assessed qualitatively, quantitatively or through a combination of both. There are aspects of personal data protection that fit into the former (i.e. risk to rights and freedoms) and the latter (e.g. data security). Quantitative risk assessment measures the probability of occurrence of a risk and combines this with its severity. Probability is expressed on a scale ranging from 0 to 1. In turn, qualitative risk assessment instead uses levels of likelihood (e.g. a quadripartite descriptive scale of negligible, low, medium, and high) to be combined with its severity. Eventually, severity of a risk indicates a magnitude of damage should a risk materialise. It can be equally expressed on a quadripartite descriptive scale. Both scales – likelihood and severity – are predefined and justified in Step 3b. A typical method for risk assessment requires, first, the identification of a risk. In the second step, the risk is analysed, for example by multiplying the likelihood (probability) of its occurrence by the severity of its consequences. In the third step, the risk is evaluated, in order to determine whether the risk and its level are acceptable, if any mitigation measure is to be recommended, and if any risk(s) should be prioritised.

Step 5b: Ethics

Analysis: The assessors analyse the recurrent arguments in the debate with specific reference to the technology under assessment, by answering the guiding questions with elaborated open answers. Along with the preliminary examples provided under the respective column, the assessors shall look into arguments:

- Appearing in newspapers, policy discourses, academic literature on the initiative (or similar initiatives), and/or
- Used by the company that produces the technology (or similar technologies), and/or
- Used by civil society organisations (e.g. activists, human rights NGOs).
- The assessors adapt each generic argument to the context of the assessment and include any relevant variations of the argument under the column 'explanation'. For every explanation, the assessors refer to the specific ID assigned in Step 2a. The assessors complete only the parts (IDs) that were ticked in Step 2a.

Assessment: The assessors determine whether the arguments identified and analysed in the analysis are sound or inconsistent. It is not necessary to complete both sub-columns under 'assessment', but at least one of them must be completed. Under the column 'assessment', the assessors might indicate:

- Whether there is any conflict between the arguments identified. For example, whether one argument contradicts another, or whether one argument is usually preferred over another (e.g. consequentialist arguments preferred to deontological or distributive justice ones). To indicate the conflicts, the assessors should use the ID numbers assigned in the previous phases.
- Whether there can be counter-arguments or fallacies to the arguments identified. The assessors use Section 5.2.3 as a guide, where for each argument possible criticisms or a list of fallacies are provided.

Step 5c: Social acceptance

Analysis: After having executed one or more social acceptance assessment techniques identified in Step 3, the assessors analyse the data collected during the previous phase, for example, if the chosen technique is a questionnaire, the assessors collect a number of completed questionnaires, be these in person or online. If the technique chosen is a workshop, participants are invited, the event is held, and minutes and/or are taken by the assessors during the event. If the technique is an interview or an observation, the assessors/interviewers take field notes and/or recordings of the discussion, and so on. which are reported again in the first column and ascribed an ID number. The 'type of analysis' can be qualitative or quantitative, or a mixture of the two, depending on the types of technique chosen. Answers obtained through close-ended questions (with scales or multiple choices) can be analysed quantitatively, using, for example, pie charts or percentages. Answers to open-ended questions involve qualitative analysis (discussion and critical analysis) *without* the use of digits and calculations.

The assessors find patterns and report a summary of findings in the final column. The findings include results that are exceptional and stand out, whereby the analysis does not simply reveal data that confirm the assessors' initial hypothesis. In the case of interviews and questionnaires, the assessors may find patterns in the replies to certain questions (e.g. some categories of travellers find the technology invasive, or the majority of interviewees find it convenient).

Assessment: The assessors assess the data analysed in the previous phase. Depending on the results, they come up with a list of (envisaged) positive and negative consequences stemming from the initiative, and specify which stakeholders are affected, and the extent to which the initiative affects them positively or negatively, by listing their names in the appropriate column.

Step 5d: Privacy

An explanatory representation of the assessment of privacy is illustrated in an 8x7 matrix, where on the vertical axis the eight types of privacy are listed (excluding informational privacy, which is equalised to data protection), and on the horizontal axis are listed the human rights limitations criteria against which these are assessed.

The assessors tick the appropriate box in the first column of the matrix (under: *Applicability* – ticking the box signifies that a certain type of privacy is assessed), and briefly describe the envisaged impact on each applicable type of privacy using factual and theoretical substantiation. Following this, and only for the applicable types of privacy under assessment, the assessors analyse each interference against human rights limitation criteria (i.e. legality, essence, necessity, proportionality, legitimacy); these criteria were elaborated in Step 5aa (cf. *supra*).

Step 5e: Legal compliance check against border management law

Analysis: The assessors evaluate whether or not the requirements listed in the table are applicable to the initiative under assessment; they may also include other requirements extracted from the legal framework applicable to the initiative, as identified in Step 2aa. An ID number (and sub-ID, when relevant) is assigned to each requirement. It is probable that not all requirements listed in the table (as extracted from the rules on EU large-scale databases, interoperability, Schengen Borders Code and Frontex Regulation) are applicable. Conversely, in cases where other rules are applicable (e.g. national laws), it may be necessary to complement the list with other requirements.

Assessment: Only if a requirement is applicable do the assessors evaluate the compliance of the initiative with the said requirement. The result of the assessment is binary (ticking or not ticking the box) because an initiative is either compliant or non-compliant with the requirement. Partial compliance is to be considered as non-compliance. In both situations, they motivate their assessment by specifying, *inter alia*, the legal and regulatory provisions from which the requirements were extracted. Reference to the legal provisions can be found in Chapter 7, in particular Section 7.5 Legal Requirements enshrining data protection, privacy and ethics in EU border management law.

Step 6: Recommendations

The goal of this Step is to provide concrete, detailed measures (controls, safeguards, solutions, etc.), their addressees and their timeframes in order to minimise the negative impacts and, if possible, to maximise the positive ones. The assessors justify their distinction between 'negative' and 'positive' impacts since this distinction is contextual and subjective. The assessor takes stock of the measures already implemented. Particularly, in the process of this integrated impact assessment, recommendations for data protection are embedded in Step 5, while for the other elements of the benchmark, a separate Step is introduced (Step 6). This choice is warranted due to the level of granularity, which is formally required by law in the case of data protection.

Data protection: By recommending possible mitigating measures, the assessors address the risks, and non-necessity and disproportionality of the processing operations in order to protect individuals and to demonstrate compliance with law. Assessors might also suggest measures to maximise positive impacts. They recommend and describe mitigation measures for each negative impact (risks, disproportionate and unnecessary interferences) identified in Step 5. Each risk is mitigated by manipulating either its likelihood (probability) – by, for example, limiting the exposure to a risk – or its severity – by, again for example, preparing a response plan should the risk materialise – or both. Risks can be

avoided, mitigated, transferred (to another entity, e.g. outsourcing, insurance, etc., or in delayed in time) or accepted. Residual risks are those that remain if there is no measure available to mitigate them and trigger a prior consultation with a supervisory authority (SA) (cf. Step 7). For both risk and non-necessity and disproportionality, mitigation measures can be of a regulatory (legal), technical, organisational or behavioural nature.

Ethics: The assessors provide recommendations on the basis of the critical evaluation of the ethical arguments identified, either to suggest how to identify (recurring) fallacies or to highlight some arguments that are side-tracked or overlooked in current policy and academic debates. For example, if an argument is not sound or is fallacious, what can be done to criticise it? What channels can be used to provide criticisms in the public debate and raise awareness? How can the public be informed of the possible risks? If two (or more) arguments are in contrast, is there a way to balance them? Which of the two arguments in contrast is the more convincing? Why? Are there any arguments that are side-tracked, suppressed, or marginalised? If so, why and by whom? If necessary, how can these 'hidden' arguments be brought to the attention of the public? If an argument is sound, and the initiative is beneficial, how can this be disseminated more effectively? Can similar initiatives be proposed in other contexts? How can this be translated into policy or new design ideas? If an argument is sound, and the initiative is harmful, how can the risks be mitigated? Are there alternative solutions in place that would be less harmful? How can this be translated into policy or new design ideas?

Social acceptance: Through the recommendations, the intention is not that the assessors ensure that the initiative is accepted, but rather that they suggest how to address the reasons of discomfort or resistance. If the assessors conclude, by contrast, that there are few reasons of discomfort or resistance, they might recommend some steps to develop or to deploy the initiative further. The assessors choose the scope and length of the recommendations, but below are some suggestions depending on the outcome of the assessment:

- If (some) travellers find the initiative acceptable and beneficial, how can these results be communicated? How can they be translated into policy initiatives?
- If (some) travellers find the initiative unacceptable and harmful, how can these harms be avoided? Is it possible to achieve the same results through less harmful means?
- If (some) travellers show different attitudes, how can these attitudes be reconciled to distribute harms and benefits more fairly?

Privacy: Given that in the previous Steps the assessors have already identified which types of privacy are applicable and to what extent they are interfered with, in this Step they introduce reverse mechanisms. Their objective is to compensate for the limitations to the right, depending on the scope of the assessment and the nature of interference (i.e. the level of intrusiveness). Such remedies could take the form of additional safeguards, transparency modalities, right of access and information forms, and explicit consent mechanisms, to be applied both before and after the use of the technology. When proposing the recommendations, the assessors shall ensure that the involved parties, including the users

of the technology, are able to be appropriately informed (at least in high-level) about the technology under assessment, its explicability, and also the meaning and function of each privacy type. There is no standard mathematical formula for assessing the risks to the right to privacy. Among best practices, it would be appropriate for the assessors to report a misalignment of the envisaged initiative and the technology involved therein, if at least one of the privacy types is unnecessarily and/or disproportionately interfered with.

Legal compliance check against border management law: When a requirement is not met, the assessors provide recommendations to ensure that the initiative is adjusted, and compliance with the requirement is achieved. The assessors use the ID and sub-ID numbers identified in the previous Step to classify the measures to be taken. The measures recommended can be technical or organisational. For example, an organisation may set up accountability measures (e.g. self-monitoring, staff-training). If the default settings of an e-gate do not respect the right to privacy, the recommendation would be to change them; if a border control technology could not be used by visually impaired persons, the recommendation would be to modify the design of the technology to make it more inclusive. The assessors conclude this Step with an implementation plan in which the responsible person, in a separate process, lists the measures and their deadline.

Upon receipt of the report, the leadership of the organisation makes a decision as to the deployment of an envisaged initiative and under what conditions.

PHASE III: EX POST (EVENTUAL) STEPS

Step 7: Prior Consultation with a Supervisory Authority

> The goal of this Step is to seek advice from an SA in the event that an impact assessment process indicates the existence of high residual risk(s) in the absence of measures taken by the data controller to mitigate such risk. Since this legal requirement is found only in data protection legislation, it essentially concerns only the first element of the benchmark pertaining to data protection.

The process of integrated impact assessment, to the extent that it incorporates a data protection impact assessment, is observed by the domestic SA. In this case, the parts on privacy, ethics and social acceptance would not be subject to review and consultation from an SA.

The communication with the SA is mainly in written form; frequently, the SA will require specific forms (templates) to request a prior consultation; the European Data Protection Board (EDPB) maintains an up-to-date contact list of its Member SAs. Insofar as an SA considers that the envisaged processing operations could infringe the law, it may provide a written notice to the data controller within a reasonable time, depending on the complexity of the request. An SA might also use its investigative and advisory powers in order to scrutinise the impact assessment process formally and substantially.

Step 8: Revisiting

The goal of this Step is to decide whether and when to perform the impact assessment process again, in its entirety or in part, under the condition that the envisaged initiative has been deployed.

Following the criteria defined in Step 3 (under 'Criteria triggering the revision of the assessment process'), the assessors perform a review of the impact assessment process when necessary. Regarding the case of data protection, this Step is performed when there is a change in the risk represented by the processing operations, i.e. if the nature, scope, context, or purpose of the processing operations have changed, and hence so has the level of risk. An impact assessment process then has to be conducted again, in total or in part.

Apart from the change in the level of risk due to a modification of a data processing operation, other factors triggering the revision process are the circumstances of the initiative's deployment, such as extending the accessibility of EU large-scale databases to more actors, the perception of social acceptance and ethics vis-à-vis a specific technology, and possibly the public pressure exercised.

ONGOING PHASE

Step A: Stakeholder involvement

The goal of this ongoing Step, which runs in parallel to each phase, is to consult (typically, seek views), throughout the entire process, if practicable, of anybody who holds a stake (interest) in the initiative, regardless of whether or not they are aware of this and of whether or not the interest is directly articulated.

Stakeholders are typically identified, informed, involved (consulted) and, eventually, have their views considered. Stakeholders whose categories have been stipulated in the Scoping Step (Step 2b) are now further identified in this Step. Their involvement is continuous, and they are asked about their views on the subject matter of each Step. Information given to stakeholders is robust, accurate, inclusive and meaningful, in plain (understandable) language, and may require the preparation of specific documentation, e.g. technical briefings. Having gathered the viewpoints of the stakeholders, the assessors consider and take a stance on their views, i.e. whether they accept them or not; if the latter, the assessors provide exhaustive justification for this. Among information, consultation, and co-decision, the choice is set at consultation, yet other levels are not excluded, should assessors deem it necessary.

Data protection: The goal of the stakeholder involvement is to consult (seek views), throughout the entire process, of data subjects and/or of their representatives as to the envisaged processing operations and privacy interferences. The exact meaning of this legal

requirement is not – and cannot be – delineated, due to the subjectivity of the term 'involvement' and the 'appropriateness' of involvement. These, in turn, depend on the degree of explicability of a given technology, on the number of relevant parties, and on the size of the project, among others.

Privacy: Beyond the formalities required by data protection legislation, a considerable number of stakeholders, with interdisciplinary backgrounds, participate in the public discourse surrounding the right to privacy. Stakeholders that are usually consulted include non-governmental organisations (NGOs) that incorporate the protection of fundamental and digital rights within the scope of their mission, the government, political parties, the police, and other authorities such as the border control authority or the ministry of internal affairs, to name a few.

Ethics: The assessors involve stakeholders in any of the previous Steps, if deemed necessary. In Step 1c, in the event that the threshold analysis questionnaire evokes a negative result (i.e. no ethics assessment is needed), the assessors consult stakeholders to confirm or oppose this outcome, to make the result of the screening more robust. In Step 2a, the assessors involve stakeholders (e.g. researchers or policy makers) to provide input as to the type of arguments present in the public debate, especially if the team of assessors does not possess enough knowledge or skills on the topic. In Step 5, the assessors involve stakeholders to carry out the analysis or to integrate or validate its results. Lastly, the assessors involve stakeholders to critically assess the arguments, support them in this task, or corroborate/criticise the assessment executed.

Social acceptance: The assessors may opt to involve additional stakeholders throughout the whole acceptance assessment process. In particular, stakeholders may provide their opinion on the validation of the results of the acceptance assessment. An example of this would be the involvement of experts (e.g. social scientists) to provide an alternative analysis of the data collected (Step 5).

Step B: Quality control

> The goal of this ongoing Step, which runs in parallel to each phase, is to check, internally and/or externally, throughout the entire assessment process, whether or not an impact assessment process adheres to a given standard of performance and to remedy, if necessary, any irregularities.

Quality control can be internal, external or both, and take the form of monitoring, review, audit, etc. The team of assessors might be required to be updated on the progress of the assessment process on a regular or *ad hoc* basis, or might establish a progress monitoring tool or an internal advisory board. The external quality control may be performed by an audit organisation hired by the data controller or, alternatively, by an SA, either upon request of the data controller or of its own volition (e.g. when required by law). The quality control can be structured, permanent or performed on an *ad hoc* basis; it can be formal

(e.g. concerning the compliance with the procedures for an impact assessment process) or substantive (e.g. if the risks were appropriately assessed). In case of judicial claims, courts of law may review an impact assessment process, either as to its form, its substance or both.

Step C: Documentation

> The goal of this ongoing Step, which runs in parallel to each phase, is to maintain intelligible records in writing or another permanent format (analogue or digital) of all activities undertaken within a given assessment process, with due respect for legitimate secrecy.

Documentation consists of the report and the attachments listed within it, both in draft and final form. Assessors also list all the activities undertaken in a given assessment process, e.g. draft versions of the report or interactions with data subjects, SAs, etc. It is best practice to make (parts of) the present report from an impact assessment process, as well as all appendices, publicly available (e.g. on the website of the data controller), with due respect for legitimate secrecy. Once the assessment process is revisited, a new version is to also be made publicly available, with reference being made within this to any previous version(s).