Smart Survey Implementation

Grant Agreement Number: 101119594 (2023-NL-SSI)

Work package 5

Design level Legal-Ethical

Deliverable 5.2: Guidelines on smart survey DPIA's with new smart features (Smart baseline stage)

Version 1.0, 2024-06-28

Prepared by:

Fabio Albo, (ISTAT, Italy) - Coordinator

Barry Schouten (CBS, The Netherlands)

Lucia Chieppa, Giovanna Cogliati Dezza, Vincenzo Palese, Tommaso Spaziani (ISTAT, Italy)

Index

1) Towards an overarching set of rules/procedures

2) Main points of Guidelines of the DPIA

3) Presentation of the template

Towards one set of rules and procedures

Ambition: Converge to a single set of decision rules and procedures to produce DPIA”s for smart surveys accepted in ESS context.

Implications:

- A need for conceptual structure, i.e. a classification of smart features and of applications
- Expanding/dynamic as more types of smart features and applications are being evaluated

What is new?

- New types of data, bringing:
  - New types of errors (accuracy gap)
  - New methods (AI-ML) leading to new processes
  - A (potential) surplus of information relative to the output need (output gap)
- Processing pushed in part to respondent devices/environment:
  - Potentially involving third parties
  - With less security and control

Towards one set of rules and procedures

DPIA's consists basically of two main parts:

1. A more objective, technical part about processes, risks, potential measures: <u>Can be connected to types of smart features</u>
2. A more subjective, ethical evaluation of added value (proportionality, purpose limitation, subsidiarity): <u>Must be viewed from the context of an application</u>

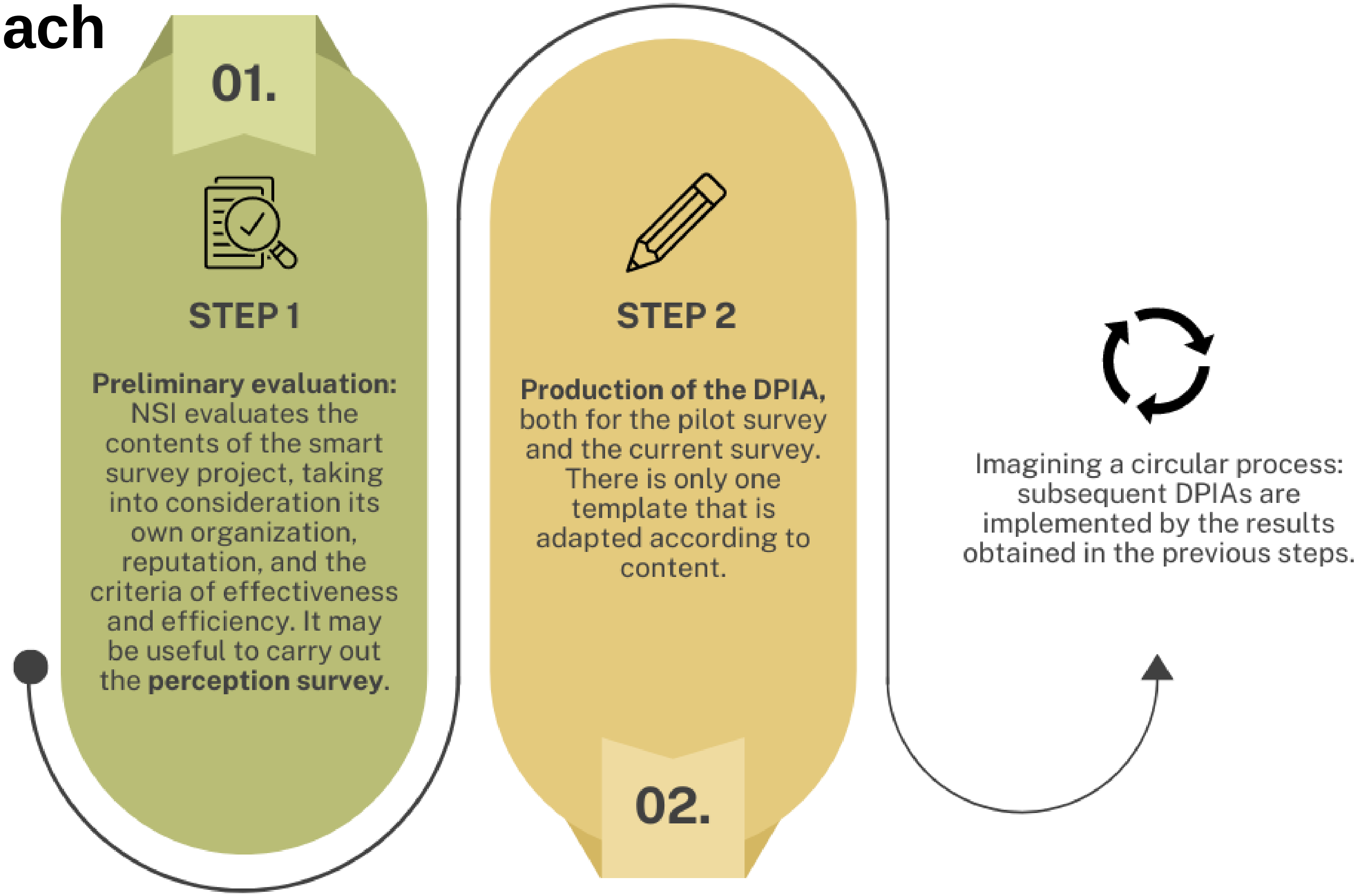
WP4 taxonomy tries to structure both parts. Criteria: Data existence, Type of measurement, Location of processing, Size of accuracy gap and Size of output gap.

Two problems:

- Accuracy gap is unknown and requires experimentation (influence, role of respondents)
- Output gap and accuracy gap lead to a friction; they have opposite needs

Problem 1: two steps approach

Within the framework of the SSI project, it was decided to use a two-steps approach in the area of privacy: the first step consists of the preliminary assessment of the appropriateness, the second step concerns the actual drafting of the DPIA - Taking in count the taxonomy and the main standard rules (GDPR, but also of the general principles contained in the European Statistics Code of Practice, and of relevant national and European legislation).



STEP 1

Preliminary evaluation: NSI evaluates the contents of the smart survey project, taking into consideration its own organization, reputation, and the criteria of effectiveness and efficiency. It may be useful to carry out the **perception survey.**

STEP 2

Production of the DPIA, both for the pilot survey and the current survey. There is only one template that is adapted according to content.

Imagining a circular process: subsequent DPIAs are implemented by the results obtained in the previous steps.

From a ‘design’ DPIA to a ‘production’ DPIA

- It is necessary to **draft the DPIA before starting data processing,** even in the case of the pilot survey
- There is **only one DPIA template**, that take in consideration data collection and data processing.
- The DPIA content changes as the results of the survey and the technological tools evolve.
- Imagining a **circular process**, looking at the first DPIA drafted (no matter if it refers to the real or the pilot survey) the subsequent DPIAs are implemented from the results obtained in the previous phases, taking into account the accuracy and output gaps calculated after every survey as well.

- Where are we?

Stage	Smart HBS	Smart TUS
Design	DE, FR, NL (+ other NSI’s)	BE, NL (travel)
Production	FI, NO	

Problem 2: Accuracy gap versus output gap

Possible solutions:

- Gain knowledge about the size of errors, the efficacy of AI-ML/methodology and the role of the respondent. It is imperative to confront the two types of ‘gaps’. Wait for the first step in the two-step approach.
- Gain knowledge about how the general population perceives a surplus of information, e.g. like in the SSI perception survey
- Establish respondent engagement
- Offer alternatives

To be further evaluated and elaborated in SSI project stage Smart Advanced

From considerations to guidelines of the DPIA

1. DPIA must be carried out by the **controller (or processor) of the personal data**. This means that the DPIA on smart surveys will have to be carried out by the individual **NSIs** and cannot be carried out at the level of the ESS.
2. The subject matter of the DPIA is the **processing of personal data through smart features**. The DPIA should assess the privacy impact of smart in the specific context of the statistical survey in which they apply.
3. The purpose of the data processing carried out through the smart features must be directly or indirectly attributable to the statistical purposes of the survey. In the DPIA, this link between the smart features and the surveys in which they are applied is necessary, from the legal point of view, to **justify the lawfulness and proportionality** of the processing of data carried out with the smart features and, from a functional point of view, to **correctly describe and evaluate the processing itself**.

From considerations to guidelines of the DPIA - continued

4. The first DPIA drafted (the pilot survey or the actual survey) is important to calculate the “accuracy gap” and the “output gap”.

The **output gap** is the difference between the output requirement of a smart survey, as specified by stakeholders and survey users, and the ideal smart data collected through the smart features used.

The **accuracy gap** is the difference between the ideal smart data not subject to any form of error and the smart data actually collected in practice.

The output gap represents a potential surplus of smart data. The accuracy gap represents the need for adjustments during the survey with the help of the respondents or post-survey adjustments without the help of the respondents. The larger the gap, the greater the **'trade-off' between data minimisation and data usefulness**. Calculating these gaps provides the opportunity to **recalibrate** and to **optimize** the next cycle of the same survey and consequently its DPIA.

5. This approach described and proposed in the SSI leads to a motivated and clearly **defined set of privacy-by-design and data-minimisation choices** for each type of smart survey.

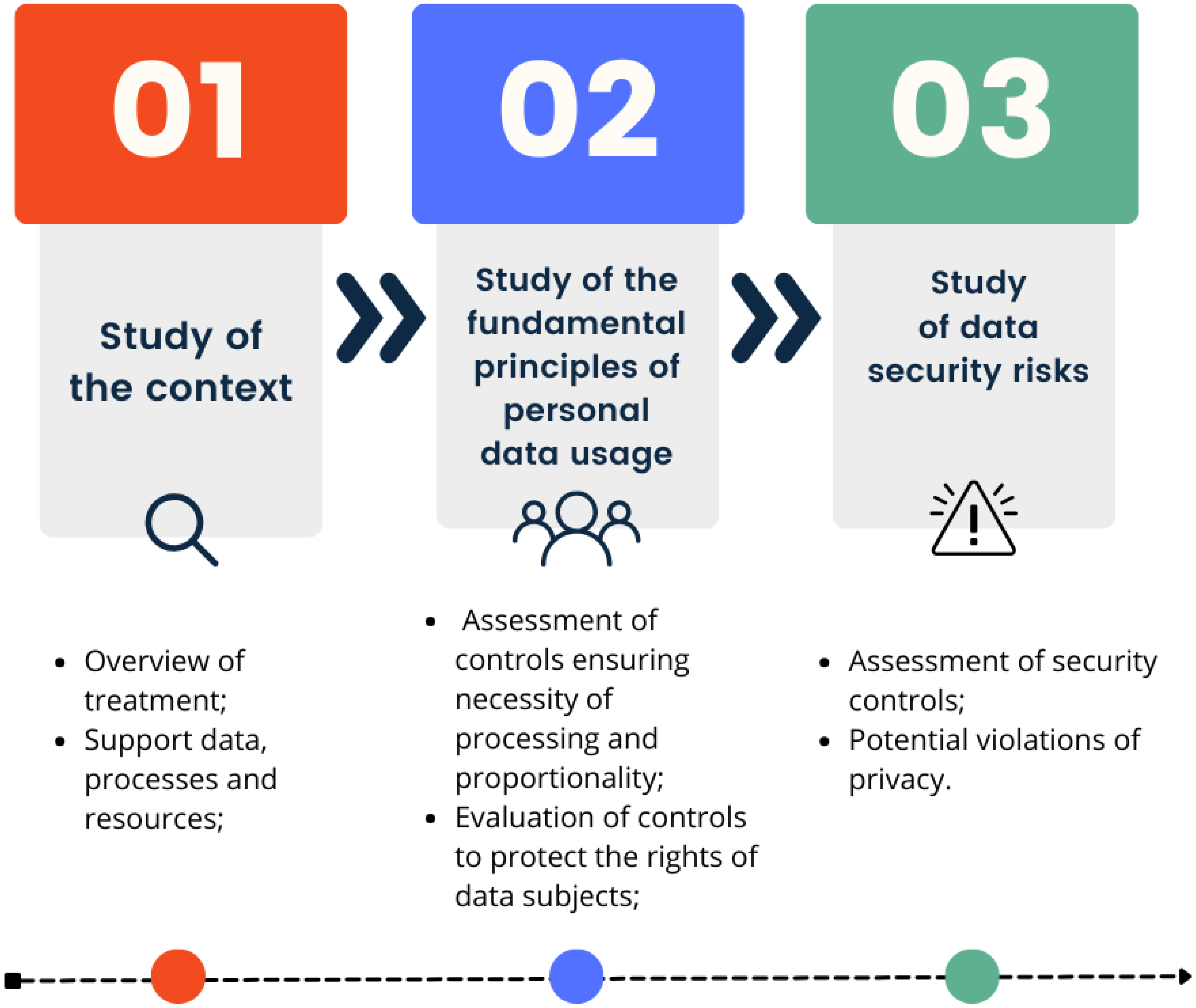
Towards rules/procedure (a template)

- There are guidelines and standards adopted by institutions that deal with the application of the GDPR that can be taken as a reference for the development of the **DPIA template for smart surveys**: the “Guidelines on DPIA” adopted by WP 29 (https://ec.europa.eu/newsroom/article29/items/611236) and the template and other tools on DPIA published by the CNIL, the French Data Protection Authority (https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil) which comply with the “Guidelines” of WP 29.

- In particular, **the DPIA template for smart surveys proposed reproduces the DPIA template of the CNIL**, adapting its structure and content to the characteristics and purposes of the processing of personal data carried out in smart surveys. Further adaptations of the template can be made by the individual NSIs that will use it in order to take into account their specificities (national legislation and policies on statistical processing, privacy, data security).

In practice

- The DPIA template proposal is focused on the **smart surveys** rather than the smart features and consists of three steps:
  1. **Study of the context, i.e. classify the features and survey**
  2. **Study of the fundamental principles of personal data usage, i.e. seek a solution to both problems**
  3. **Study of data security risks, i.e. make decisions given experiences for a type of smart survey**



01

Study of the context

- Overview of treatment;
- Support data, processes and resources;

02

Study of the fundamental principles of personal data usage

- Assessment of controls ensuring necessity of processing and proportionality;
- Evaluation of controls to protect the rights of data subjects;

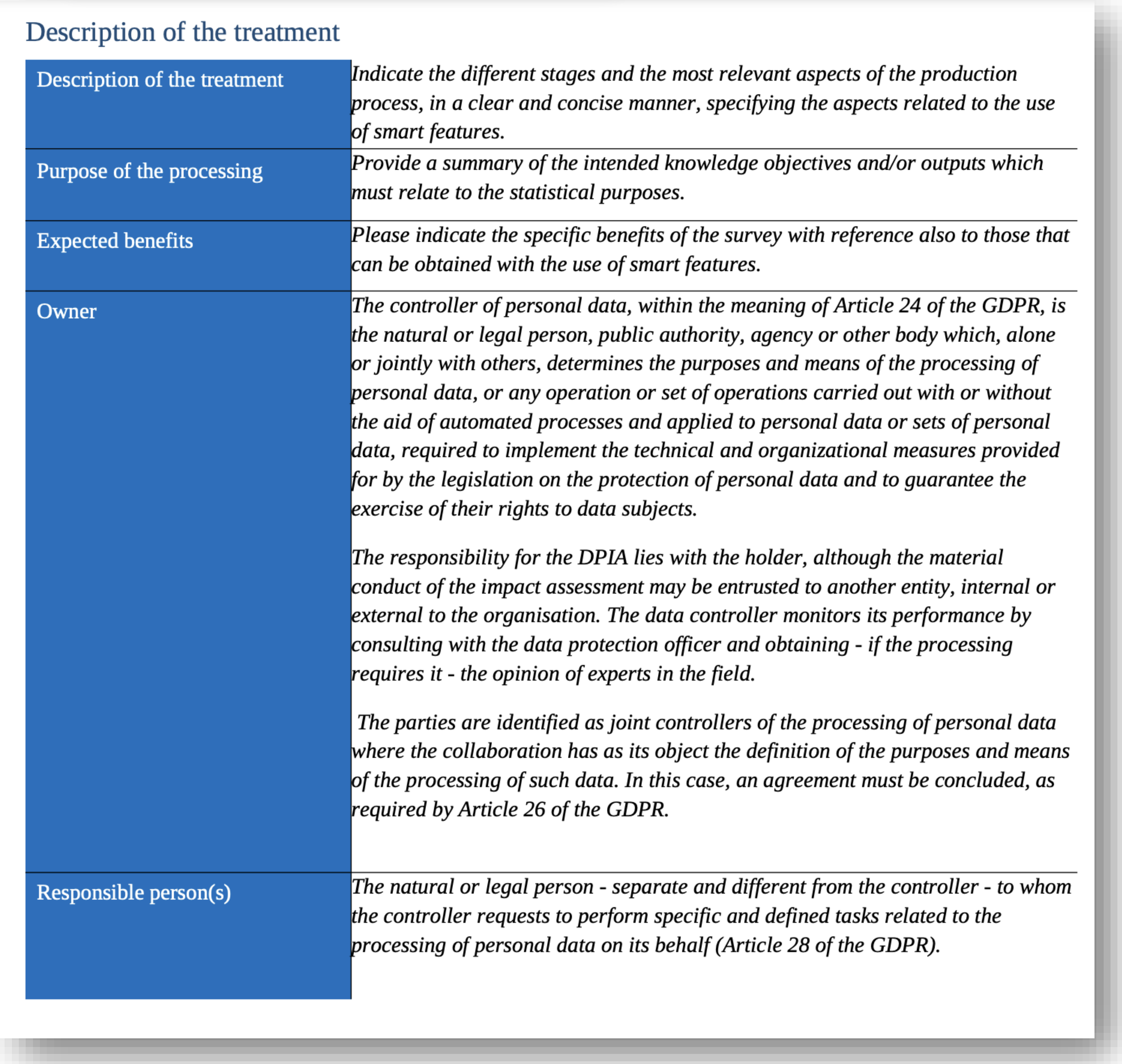
03

Study of data security risks

- Assessment of security controls;
- Potential violations of privacy.

Template preview: Study of the context

This section concerns the **description of the treatment** and it must be filled out indicating the controllers and possibly the joint controllers and processors, within the meaning of the GDPR, considering that also for the use of smart features the involvement of parties external to the controller must comply with these regulatory references if it involves the processing of personal data.

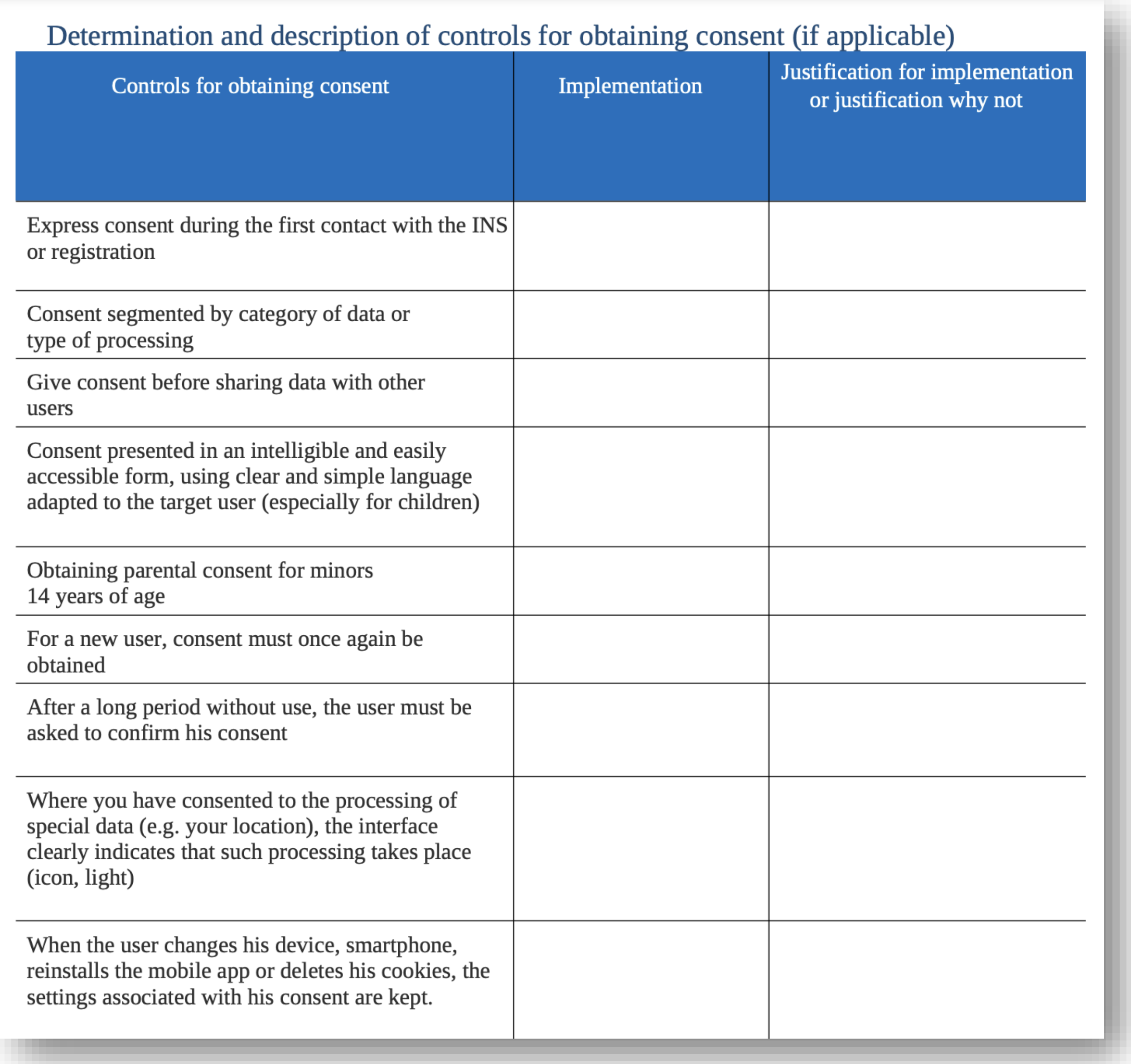


Description of the treatment

Description of the treatment	*Indicate the different stages and the most relevant aspects of the production process, in a clear and concise manner, specifying the aspects related to the use of smart features.*
Purpose of the processing	*Provide a summary of the intended knowledge objectives and/or outputs which must relate to the statistical purposes.*
Expected benefits	*Please indicate the specific benefits of the survey with reference also to those that can be obtained with the use of smart features.*
Owner	*The controller of personal data, within the meaning of Article 24 of the GDPR, is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data, or any operation or set of operations carried out with or without the aid of automated processes and applied to personal data or sets of personal data, required to implement the technical and organizational measures provided for by the legislation on the protection of personal data and to guarantee the exercise of their rights to data subjects.* *The responsibility for the DPIA lies with the holder, although the material conduct of the impact assessment may be entrusted to another entity, internal or external to the organisation. The data controller monitors its performance by consulting with the data protection officer and obtaining - if the processing requires it - the opinion of experts in the field.* *The parties are identified as joint controllers of the processing of personal data where the collaboration has as its object the definition of the purposes and means of the processing of such data. In this case, an agreement must be concluded, as required by Article 26 of the GDPR.*
Responsible person(s)	*The natural or legal person - separate and different from the controller - to whom the controller requests to perform specific and defined tasks related to the processing of personal data on its behalf (Article 28 of the GDPR).*

Template preview:
Study of the fundamental principles of personal data usage

This section concerns the evaluation of controls to **protect the rights of data subjects** and focuses on the description of the measures for obtaining **consent**, how they are implemented and the justification for eventuale implementation.

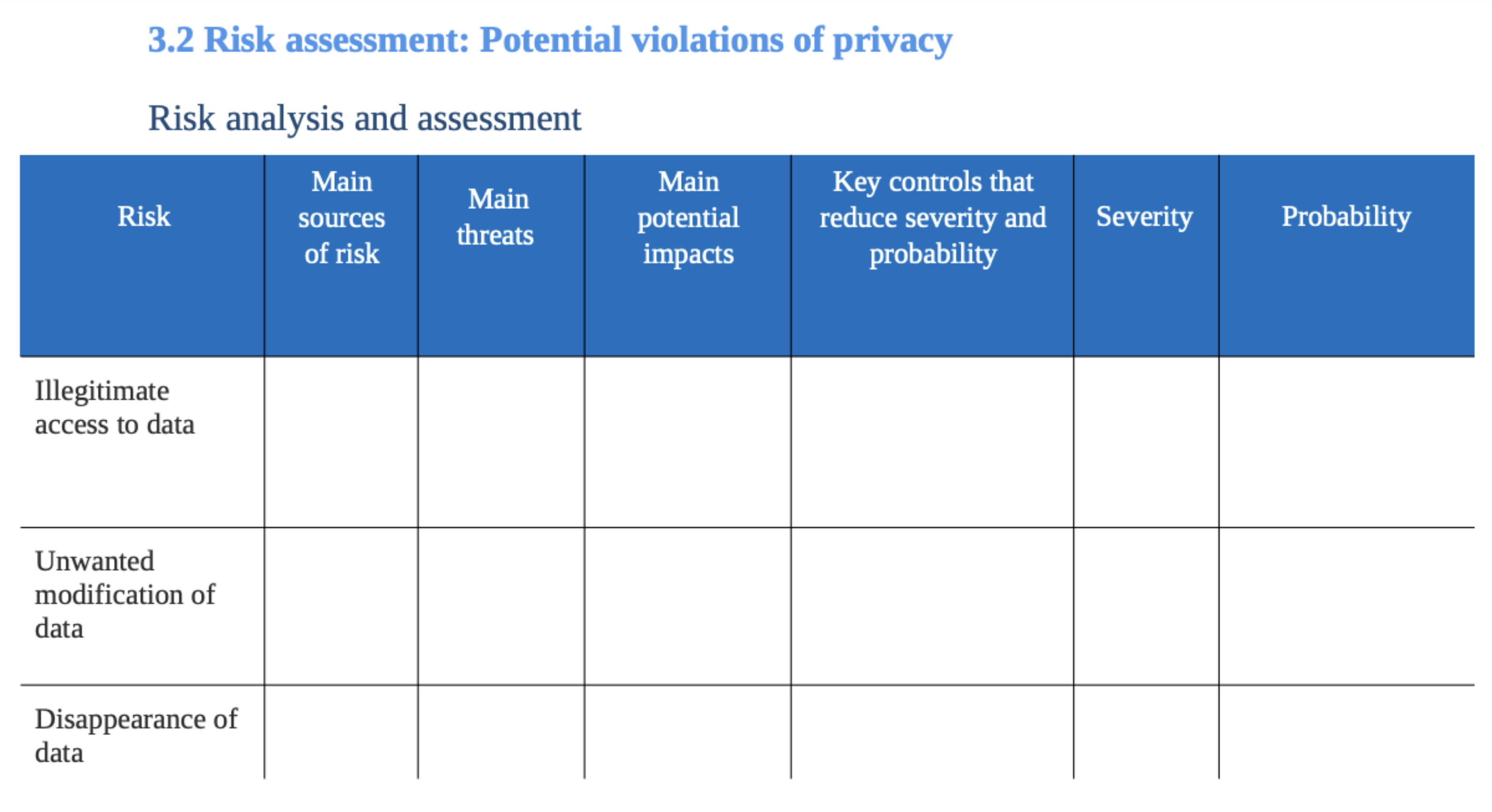


Determination and description of controls for obtaining consent (if applicable)

Controls for obtaining consent	Implementation	Justification for implementation or justification why not
Express consent during the first contact with the INS or registration		
Consent segmented by category of data or type of processing		
Give consent before sharing data with other users		
Consent presented in an intelligible and easily accessible form, using clear and simple language adapted to the target user (especially for children)		
Obtaining parental consent for minors 14 years of age		
For a new user, consent must once again be obtained		
After a long period without use, the user must be asked to confirm his consent		
Where you have consented to the processing of special data (e.g. your location), the interface clearly indicates that such processing takes place (icon, light)		
When the user changes his device, smartphone, reinstalls the mobile app or deletes his cookies, the settings associated with his consent are kept.		

Template preview:
Study of data security risks

This section on **risk analysis and assessment** requires the study of potential privacy breaches, providing an answer on the main sources of risk, threats, impacts, etc.



3.2 Risk assessment: Potential violations of privacy

Risk analysis and assessment

Risk	Main sources of risk	Main threats	Main potential impacts	Key controls that reduce severity and probability	Severity	Probability
Illegitimate access to data						
Unwanted modification of data						
Disappearance of data						

Additional general indications:

- **Evaluation of Processing Activities**: The DPIA should describe in detail how the extended smart features will process personal data, including the types of data collected, the methods of collection, the basis for processing, the respondents affected, and the intended use of the data.

- **Proportionality**: The DPIA should practically considerate if the added value of including a smart feature(s) outweigh the privacy intrusion. In the preliminary opportunity assessment stage, instead, proportionality is addressed to evaluate, from a theoretical point of view, the burden on respondents.

- **Risk Assessment**: The DPIA should identify and assess risks to the rights and freedoms of natural persons that may arise from the use of the smart features, including potential for data breaches, profiling, or other privacy-invasive activities.

- **Mitigation Measures**: The DPIA should outline measures to mitigate identified risks, ensuring that the privacy impact of the smart features is minimized.

- **Link between Features and Survey**: There must be a clear link between the smart features and the surveys in which they are applied.

Additional general indications:

- **Documentation and Accountability**: The DPIA should be thoroughly documented, providing a clear rationale for the introduction of smart features, the expected benefits, and how any associated risks are being addressed. This documentation is essential for demonstrating compliance with GDPR requirements.
- Smart feature(s) **security risks** and per risk chances of occurrence, **consequences and mitigation measures** (including *PET Privacy-enhancing technologies*).
- Use **of third parties software applications**, **sensors or devices** with enabled smart features and the third parties involvement in the process, also considering agreements that bind them to the NSI.
- **Data minimisation and privacy-by-design**: The smart survey should follow the principles of data minimisation and privacy-by-design and the DPIA should describe how these principles are applied.
- Inclusion **of special category personal data** or personal data relating to criminal convictions and offences: The DPIA should thoroughly describe, as provided for by Article 9 and 10 of GDPR, the need and the treatment of special category personal data or personal data relating to criminal convictions and offences and the security measures applied to protect these data

Thank you!