











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)

Work package Leader:

Fabio Albo (ISTAT, Italy)
e-mail address : albo@istat.it
mobile phone : +39 3490424519

Index

Summary

This report describes the activities carried out by the Working Group regarding the definition of 'Guidelines' for the development of a DPIA on smart surveys.

We structure the document as follows: section 2 contains a glossary with definitions related to the smart surveys developed within the SSI project; section 3 recalls the main standard rules on DPIA in official statistics; section 4 describes the approach to be followed in the implementation of DPIA in smart surveys; finally, section 5 presents the DPIA template for smart surveys, which is attached as a separate document (Annex A).

1. Introduction

From a legal perspective, the ultimate goal is to create one overarching DPIA for ESS-surveys that employ one or more smart features from a specified set of smart features. The emphasis on a set of smart features is made because new features may be developed and/or added gradually in time. It is the task of project SSI to create a first overarching DPIA for features used in the three SSI case studies receipt processing, geo-tracking and energy meter data donation. Given that in time more features and more applications will be added, the general DPIA will, by nature, be a dynamic document.

In order to achieve this objective, we consider it useful first of all to elaborate and propose a template that can be used for the realisation of DPIAs on smart surveys.

The template is accompanied by instructions on how to complete the DPIA and is based on definitions, standards, and considerations that will be set out in the following paragraphs.

Together these elements constitute a first proposal for "Guidelines on the DPIA of the smart surveys with new smart features".

2. Definitions

Within the Smart Survey Implementation (SSI) project, three smart services were developed, implemented, tested and evaluated: receipt processing, geo-tracking and energy meter data donation.

Definitions are listed to better frame these concepts and to facilitate the reading of this document.

Smart feature: A smart feature is a data collection action through a smart device such as:

- In-device storage and/or computing
- Employment of in device-sensors
- Linkage to external sensor systems
- Linkage to public online data
- Data donation through the respondent
- Data donation through the statistical institute, i.e. requiring identification keys to link data already in possession

***Smart data*:** Smart data are data collected through one or more smart features;

Smart task: A smart task is a processing action applied to smart data;

Smart service/solution: A smart service is a combined and implemented series of smart tasks (i.e. with a single input and a single output);

Geo-tracking: smart feature that identifies a person's current physical location by obtaining GPS data from their smartphone or other GPS-enabled devices;

Device: hardware unit, electronic device; in particular, high-tech and small devices;

Sensor: a device that interacts with the quantity to be measured and its environment and detects its variations;

Passive data collection: involves gathering data without active participant involvement and is well-suited for continuous, objective data;

Active data collection: relies on participants actively providing data and is used for subjective information and specific insights.

Sources: These are additional data about respondents or groups of respondents, used as features in methods for cleaning, editing, imputing, predicting, or transforming data. Sources come in two forms:

1. Data already possessed by the institute (e.g., administrative data).
2. Linkage of public online data, which may require preprocessing and editing.

Actors: Individuals involved, who may be the respondent themselves and/or data collection staff.

Rules: These depend on the task type and serve as input parameters to the methods employed within the task.

Standards: These are lower thresholds for smart data quality. If the quality falls below these thresholds, the task cannot be performed. This may necessitate re-initiating a preceding smart task or requiring additional respondent context or supplements.

Tools: These are task-dependent and comprise external methods validated in the literature, such as libraries or packages.

Learning: This involves using the output data of the smart task to adapt to individuals or groups of respondents. If this is applied, the smart task output must specify which data needs to be set aside for learning purposes.

For further considerations, please refer to the taxonomy document prepared by WP 4.

3. Main standard rules

When defining and applying the DPIA Guidelines on smart surveys, reference must first be made to the principles and rules of the GDPR, especially those concerning processing for statistical purposes.

Article 5 (Principles relating to processing of personal data) provides that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')[...];

Article 6 (Lawfulness of processing) provides that processing shall be lawful if [...] is necessary for the performance of a task carried out in the public interest or in exercise of official authority vested in the controller.

Article 9 (Processing of special categories of personal data) provides, as well, that processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation is authorized if it is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Article 89 (Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes) provides that these kind of processing shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not

permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15 (Right of access by the data subject), 16 (Right to rectification), 18 (Right to restriction of processing) and 21 (Right to object) subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.
3. […]
4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.

Finally, regarding procedural aspects, Article 35 (Data protection impact assessment) provides as follows:

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

Article 36 (Prior consultation) provides that the controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

When drafting the DPIA relating to the processing of personal data for official statistical purposes, account must be taken not only of the GDPR, but also of the general principles contained in the European Statistics Code of Practice, and of relevant national and European legislation

The processing purposes of the smart features must align with the overall purposes of the survey. The DPIA should examine whether the processing is lawful under the GDPR and whether it is proportionate to the aims pursued. This means that the benefits of using the smart features should outweigh any potential risks to the respondents' privacy.

4. Considerations for drafting DPIAs for the treatment of personal data in smart surveys

Within the framework of the SSI project, it was decided to use a two-step 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.
From a procedural point of view, we will structure the creation of two-step procedures: a first step must take into consideration the ethical and institutional aspects related to the choice of using intelligent functionalities, and a second step concerns the actual drafting of the DPIA.
The articulation of the process in these two steps is necessary because the processing of personal data cannot be started before the DPIA is completed, and the DPIA, even if aimed at design, cannot have an abstract and hypothetical object, but must consider real personal data processing, the tools and purposes of which must be described and assessed in detail.

PRELIMINARY OPPORTUNITY ASSESSMENT
The preliminary opportunity assessment has to take into consideration the political-institutional aspects linked to the choice of using smart features of any kind and per se, referring both to the official statistics regulations (European, national, etc.) and to the policies of the individual NSIs (i.e. ethics committee, additional cybersecurity rules, public image consideration).
In particular, the issues an NSI has to address at this stage are:

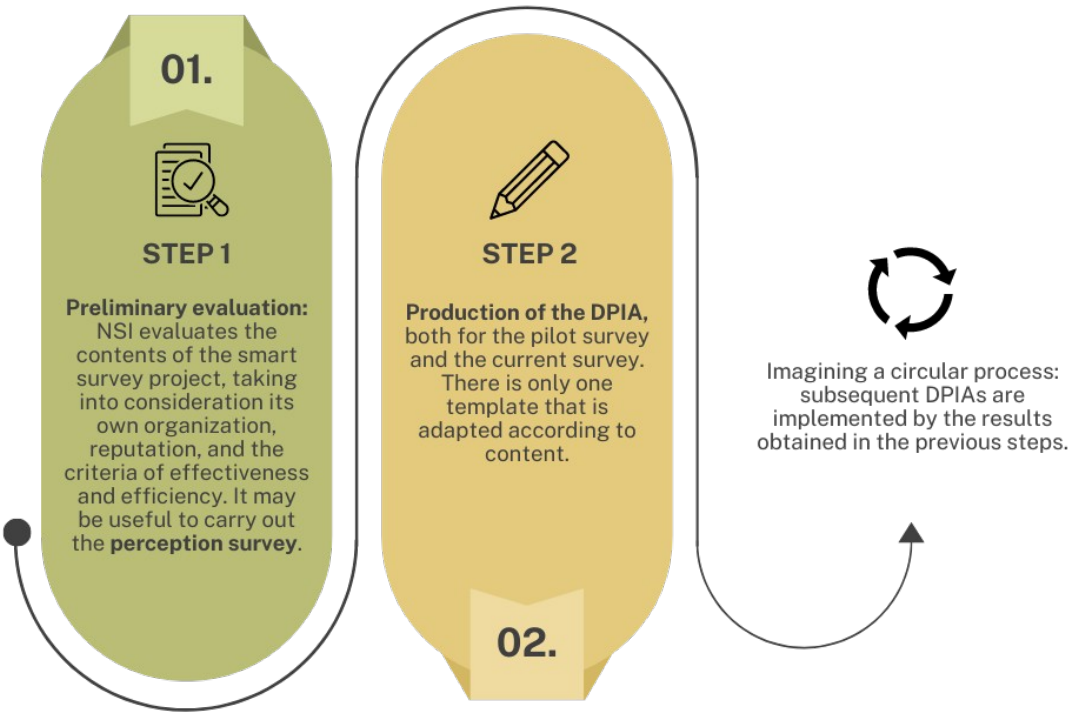
- Motivation for use of smart feature(s)
- Subsidiarity (is there no reasonable alternative for the smart feature(s) that will be less intrusive and/or risky?)
- Purpose limitation (are the data purely intended for primary use in offstats?)
- Proportionality (does the added value of including a smart feature(s) outweigh the burden?)

Furthermore, it may be useful to realize a perception survey on the subject to obtain more information regarding the involvement of the respondants and their data impact perception.

DATA PROTECTION IMPACT ASSESSMENT

Once the opportunity has been established to use of smart features, it is necessary to draft the DPIA before starting data processing, even in the case of the pilot survey. If in the previous stage the NSI had to decide whether to use smart features or not, now it has to decide how (and how strongly) to use them. There is only one DPIA template, both for the pilot and for the production, that take in consideration data colletction 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.

The following table represents the two steps and the necessary 'circularity' of the DPIA:


01.
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.
02.
Imagining a circular process: subsequent DPIAs are implemented by the results obtained in the previous steps.

5. DPIA template introduction

The GDPR does not formally define the concept of a data protection impact assessment and does not indicate a unique way to carry it out, but defines its minimum content (Article 35(7)). Furthermore, no templates or guidelines on how to conduct a DPIA for the processing of personal data in the context of statistical surveys have been formally adopted under the ESS. However, 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).

The development of the DPIA template for smart surveys that we propose is based on the following considerations:

1) The DPIA template proposal is focused on the smart surveys rather than the smart features and consists of three parts: Study of the context, Study of the fundamental principles of personal data usage, Study of data security risks.

2) DPIAs 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. The proposed DPIA template on smart surveys is made for use by individual NSIs that will carry out smart surveys using one or more "smart features" developed under the SSI project. This assumption leads one to reconsider the meaning and feasibility of a general DPIA on smart surveys. In fact, a general DPIA carried out in the context of the ESS and which does not deal with specific applications would be conceptual and abstract in nature and therefore could not constitute a legally valid prerequisite for the processing of personal data. Common assessments, tools, rules and procedures may be developed and proposed in the ESS context, but the actual DPIA conduct is the responsibility of the NSI and requires assessing smart functions in the context of individual surveys.

3) Examination of the experiences of the NSIs in the various countries shows that separate DPIAs are usually carried out for standard processing operations with common characteristics (e.g. processing operations concerning current surveys using the same techniques and methods of data collection and processing) and for non-standard processes (e.g. when new techniques and methods are introduced into a standard processing operation). The template considering smart surveys as a non-standard treatment. The template applies in fact to the case where new techniques and methods (the "smart

features") are introduced within a statistical survey already planned and currently carried out by the NSIs of the ESS (e.g. TUS), which therefore has a predefined statistical purpose and legal basis. Only relative changes to existing data collections through the smart services are considerated: this means, implicitly, that are not take into account data collections that produce entirely new statistical output.

4) The subject matter of the DPIA is not smart features as such, but the processing of personal data through smart features. Therefore, the DPIA should assess the privacy impact of smart features not "in the abstract", but in the specific context of the statistical survey in which they apply. The reference to the specific context of the survey is indeed crucial to correctly describe and assess in the DPIA the data processing carried out through smart features. 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, they cannot be considered autonomous. 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.
5) Smart features, and the resulting smart data, are evaluated through the two-step approach within a circular process described before: the first step is the preliminary opportunity assessment; the second one is the actual DPIA.
   The first DPIA drafted (referring to 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.
6) The types of features and smart surveys evaluated are gradually expanded over time, leading to a growing body of risk assessment and data minimisation procedures.

The proposed DPIA template should be completed taking into account these 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 minimised. This could include technical and organisational measures like data minimization, pseudonymization, encryption, privacy enhancing technologies such as secure multi parti computation access controls, and transparent respondent communication.
- Link between Features and Survey: There must be a clear link between the smart features and the surveys in which they are applied. This link is crucial for justifying the processing activities both legally and functionally. It ensures that the respondents understand the context in which their data is being processed and the reasons for it.
- 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.

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)

DPIA TEMPLATE FOR SMART SURVEYS

Warnings

For the compilation of this DPIA template, it is also necessary to take into account the general indications contained in the document "Guidelines on the DPIA of smart investigation with new smart functionalities (smart basic phase)"

Specific indications are given in italics.

A general rule is to represent the specific measures adopted in implementation of the regulatory principles avoiding mere repetitions of obligations already provided for by the GDPR and assertions of compliance with the GDPR itself.

The DPIA drafting process is iterative: in practice, each of the steps is likely to be reviewed several times before the data protection impact assessment can be completed.

Regulation (EU) 2016/679 is indicated GDPR.

Website:

https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-pia-2-en-templates.pdf

https://www.cnil.fr/en/english-french-glossary-data-protection

https://www.cnil.fr/fr/glossaire/d

1 Context study

1.1 Overview of treatment

Enter the description and purpose in introductory terms, highlighting the most relevant aspects and taking into account the additional elements that are specified in the subsequent relevant parts of the document – indicate 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).*

Sectoral rules applicable to processing

Insert the provisions of international, European and national regulations that have as their object the definition of the methods of statistical work. More specifically, it is necessary to

consider the rules identifying the purpose of official statistics pursued by the survey. Due account must be taken of compliance with the codes of conduct – where they have been approved – set out in Article 40 of the GDPR.

Rules applicable to processing	Considerations
Please insert the legal references that constitute the legal basis for the processing of personal data for the pursuit of the purposes of the investigation also irrespective of the use of smart features (considering that there is no autonomous legal basis for the use of smart features).	
Check whether other regulatory references are relevant in view of the subject matter of the investigation and the use of smart features.	

1.2 Support data, processes and resources

Description of data, recipients and storage times

Enter the different types of personal data processed in consideration of the nature of personal data and specific objects, indicate the persons in charge of the processing and the storage time in light of the limitation principle provided for by the GDPR

Types of data	Contact persons/processors	Duration of storage
Specify whether personal data is processed		*Indicate the storage time in a specific way (e.g. in months or in relation to the occurrence of a specific event).*
Please indicate the subject of the personal data using categories: e.g. identification data (e.g. account); personal data; location data; contact details; Education/training data; income data; data relating to the employment situation; ...		
Specify whether particular categories of data or judicial data are processed (Articles 9 and 10 of the GDPR)		
Indicate which data are processed anonymously (e.g. Tracking not associated with other information)		

Description of supporting processes and resources

[Insert a detailed description of the processes carried out by identifying the actors and the different roles, highlighting the link with the possible public interest and/or the legal obligations

pursued – indicate which resources (e.g. IT, hardware, software) are used and the type of smart features, also taking into account the taxonomy defined within the project – highlight the aspects that justify or - better - that suggest the use of smart features (for example when the use is closely linked to the production of data, as for electricity meters) – it is useful to describe the step by step process and insert a flow diagram

Processes	Detailed description of the process	Support resources

2 Study of fundamental principles

2.1 Assessment of controls ensuring necessity of processing and proportionality

Explanation and justification of the purpose

Purpose	Legitimacy
Please indicate the specific statistical purpose pursued by the survey and the benefits achieved through the use of smart features.	*Please indicate the legal basis of the investigation considering that the use of smart features does not have a different and autonomous one.*
Example: Geotracking in TUS *Geotracking can be used in three ways in TUS:* *Create a day roster/overview consisting of travel and stops. The start - end times are known to be very helpful anchor points for respondent to fill in the diary. TUS has a time resolution of 10 minutes and includes all possible types of activities. This means there cannot be blanks in the diary. In practice, respondent do not walk around with the diary in hand and fill in at the end of the day or at best a few times a day. The stop-track reminds them. It must be noted that geotracking data are just a series of location points. Constructing stops from these points is not so straightforward and requires all kinds of decision rules. Predict transport modes. TUS respondent need to supplement travel time slots with the main transport modes. This is burdensome for them, especially when they use multiple modes. Based on derived characteristics from location data such as speed, acceleration and vicinity to so-called open points-of-interest data, likely modes can be predicted. Activity/stop purpose prediction: The main target of TUS is activity. While this is can be very different when people are at home, certain locations are connected to certain activities (shops, cinema, park, museum, etc). With points-of-interest data it is predicted for certain types of locations what is the likely activity.*	

Explanation and justification of legality

Please specify the following legitimacy criteria and any specific procedures for requesting consent step by step in the use of smart features:

Legality criteria	Applicable	Justification
The interested party has given consent to the processing of their personal data for one or more specific purposes		
Processing is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject before entering into a contract		
The processing is necessary for the fulfillment of a legal obligation to which the controller is subject		
Processing is necessary to protect the vital interests of the data subject or another natural person		
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 controller		
Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, unless the interests or fundamental rights and freedoms of the data subject which require the protection of personal data prevail, in particular where the data subject is a minor.		

[4] This point shall not apply to processing operations carried out by public authorities in the performance of their duties.

Explanation and justification of data minimisation

Insert for the personal data indicated in line with what has already been stated in point 1.2 the justification of the necessity and relevance

Details of the data processed	Data categories	Justification of the necessity and relevance of the data	Minimisation checks
		Highlight the elements of assessment that led to the conclusion that such data processing was necessary, balancing the consequent utility/advantage with respect to the sacrifice of the rights of the data subject. *For example, when the type of data is closely linked to the use of smart features, such as for electricity meters in the field of energy statistics.*	*Please indicate the elements of balancing assessment and the measures taken to make the treatment as non-invasive as possible.* *For example, it may be useful to point out that this is a pilot survey and, therefore, that the sacrifice due to the processing of more data is justified by the fact that these data are processed exclusively for quality control purposes and for a limited time in order to achieve a higher level of precision and proceed with the survey in production by limiting the data collected. In relation to the use of identification data (e.g. account, URL), for example, highlight the need only for certain precision and quality purposes and using encryption techniques.*

Explanation and justification of data quality

Insert a description of the quality controls adopted, highlighting the elements necessary to justify an increased risk in line with the previous paragraph

Data quality checks	Justification

Explanation and justification of retention periods

Indicate the storage time in a specific way (e.g. in months or in relation to the occurrence of a specific event). Pay attention to the justification of the storage time for both too short and too long times, clarifying the reasons in relation to the type of data and the protection measures adopted (for the particular categories of data or identification data indicate short times linked to specific and necessary cognitive needs, highlighting the encryption and pseudonymization techniques preferably to be used).

Types of data	Duration of storage	Justification of the shelf life	Deletion mechanism at the end of the retention period
Common data			
Archived data			
Functional traces			
Technical registers			

Assessment of controls

The representation of the information described so far must be integrated with that of the subsequent information in order to highlight the elements of assessment first with reference to the principle of necessity: in view of the description of the processing, it is necessary to highlight the elements of assessment that led to the conclusion that this tool was more useful/advantageous and as less invasive of fundamental rights and freedoms as possible – and then the elements of assessment of the principle of proportionality in view of the importance of the objective to be achieved and the way in which the investigation intends to pursue it in relation to the sacrifice of the rights of the data subject and any measures put in place to limit that sacrifice

Controls ensuring proportionality and necessity of processing	Is it acceptable/can it be improved?	Corrective checks
Purpose: specified, explicit and legitimate		
Base: lawfulness of processing, prohibition of misuse		
Data minimisation: adequate, relevant and limited		
Data quality: accurate and up-to-date		
Duration of storage: limited		

2.2 Evaluation of controls to protect the rights of data subjects

Determination and description of controls for information purposes for data subjects

If the processing benefits from an exemption from the right to information, as provided for in

Articles 12, 13 and 14 of the [GDPR]:

Exemption from the obligation to inform data subjects	Justification

Otherwise:

Controls for the right to information	Implementation	Justification for implementation or justification why not
Presentation of Terms & Conditions of Use/Confidentiality		
Possibility to access the terms & conditions for use / confidentiality		
Readable and easy-to-understand terms		
Existence of device-specific clauses		
Detailed presentation of the purposes of the data processing (specific objectives, correspondence of the data, where applicable, *etc.)*		
Detailed presentation of the personal data collected		
Presentation of any access to device identifiers specifying whether these identifiers are disclosed to third parties		
Presentation of the user's rights (withdrawal of consent, deletion of data, *etc.)*		
Information on the method of secure storage of data, in particular in the case of procurement		
How to contact the holder (identity and contact details) on confidentiality issues		
Where applicable, information for the user on any changes regarding the data collected, the purposes and the confidentiality clauses		

Controls for the right to information	Implementation	Justification for implementation or
With regard to the transmission of data to third parties:		
- detailed presentation of the purpose of the transmission to third parties		
- detailed presentation of the personal data transmitted		
- indication of the identity of the third-party bodies		

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.		

Determination and description of controls for access rights and data portability

If the treatment benefits from an exemption from the right of access, as provided for

Article 15 of the [GDPR]:

Exemption from the right of access	*Justification*	*How to respond to data subjects*

Otherwise:

Controls for the right of access	Internal data	External data	Justification
Possibility to access all the user's personal data, through the common interfaces			
Ability to safely consult the traces of use associated with the user			
Possibility to download an archive of all personal data associated with the user			

Finally, if the right to data portability applies to the processing pursuant to Article 20 of the [GDPR]:

Checks for the right to data portability	Internal data	External data	Justification
Possibility of retrieving, in an easily reusable format, the personal data provided by the user, in order to transfer them to another service			

Determination and description of controls for rectification and erasure rights

Where the processing benefits from an exemption from the right to rectification and erasure, as provided for in Article 17 of the [GDPR]:

Exemption from the right to rectification and erasure	Justification	How to respond to data subjects

Otherwise:

Controls for rectification and erasure rights	Internal data	External data	Justification
Possibility of rectification of personal data			
Possibility of deletion of personal data			
Indication of the personal data that will still be stored (technical requirements, legal obligations, *etc.)*			
Implementation of the right to be forgotten for children			
Clear instructions and simple steps for deleting data before the device is scrapped			
Tips on Restoring Your Device Before Selling It			
Ability to delete data in case of device theft			

Determination and description of controls for restriction of processing and objection rights

If the processing is exempted from the right to restriction and to object, as provided for in or under Article 21 of the [GDPR]:

Exemption from the right of restriction and opposition	Justification	How to respond to data subjects

Otherwise:

Controls for restriction and opposition rights	Internal data	External data	Justification
Existence of "Privacy" settings			
Invitation to change default settings			
"Privacy" settings accessible during registration			
"Privacy" settings accessible after registration			
Existence of a parental control system for children under the age of 13			
Tracking compliance (cookies, advertising, *etc.)*			
Exclusion of children under 13 from automated profiling			
Effective exclusion of the processing of user data in case of withdrawal of consent			

Determination and description of controls applicable to controllers

Name of the person responsible	Purpose	Scope	Contract reference	Compliance with Art. 28[6]

[6] A processing contract must be signed with each controller, which defines all the aspects provided for in Article 28 of the [GDPR]: duration, scope, purpose, documented processing instructions, prior authorisation in case of recruitment of a controller, provision of any

documentation demonstrating compliance with the [GDPR], timely notification of any data breach, *etc.*

Determination and description of controls on data transfer outside the European Union

Data set and storage location	EU Member State	Country recognised as providing adequate protection by the EU	Other country	Justification and supervision (standard contractual clauses, company internal regulations)

Assessment of controls

Controls to protect the rights of data subjects	Is it acceptable/can it be improved?	Corrective checks
Information for data subjects (fair and transparent treatment)		
Obtaining consent		
Exercise of access rights and data portability		
Exercise of the rights of rectification and cancellation		
Exercise of the rights of limitation of processing and opposition		
Data processors: identified and governed by a contract		
Transfers: fulfillment of obligations related to the transfer of data outside the European Union		

3 Study of data security risks:

3.1 Assessment of security controls

Description and evaluation of controls implemented for the treatment of risks related to the safety of data. With reference to smart surveys, the following risks must be considered as a priority:

Systematic and extensive profiling of individuals in a detailed or extensive manner

Large scale processing of sensitive data

Systematic monitoring of public areas

Controls that specifically concern the data being processed	Implementation or justification why not	Is it acceptable/can it be improved?	Corrective checks
Encryption	*Describe here the means put in place to ensure the confidentiality of the data stored (in the database, in flat files, in backups, etc.), as well as the procedure for managing encryption keys (creation, storage, modification in case of suspected cases of data compromise, etc.).* *Describe the encryption means used for the data streams (VPN, TLS, etc.) implemented in the processing.*		
Anonymisation	*Please indicate here whether anonymisation mechanisms are implemented, what and for what purpose.*		
Data partitioning (in relation to the rest of the information system)	*Indicate here whether partitioning is to be processed, and how this happens.*		

Logical access control	*Indicate here if user profiles are defined and attributed.* *Specify the means of authentication implemented.* *If applicable, specify the rules applicable to passwords (minimum length, characters required, duration of validity, number of failed attempts before access to the account is blocked, etc.)*		

Controls that specifically concern the data being processed	Implementation or justification why not	Is it acceptable/can it be improved?	Corrective checks
Traceability (registration)	*[Indicate here if events are recorded and how long these tracks are stored*		
Integrity monitoring	*[Indicate here if mechanisms for monitoring the integrity of stored data are implemented, what and for what purpose.* *Specify which integrity control mechanisms are implemented on the data flows.]*		
Archiving	*[Describe here the processes of archive management (delivery, storage, consultation, etc.) under the responsibility of the owner. Specify the archiving roles (source offices, transferring agencies, etc.) and archiving policy.* *Indicate whether the data may fall within the scope of public repositories.]*		

Description and assessment of general security controls

General security checks relating to the system in which the processing is carried out	Implementation or justification why not	Is it acceptable/can it be improved?	Corrective checks
Operational security	[*Describe here how software updates (operating systems, applications, etc.) and the application of corrective security controls are carried out.*]		
Blocking malicious software	[*Indicate here if an antivirus software is installed and updated at regular intervals on your device*]		
Backup	[Indicate*here how backups are handled. Clarify if they are stored in a safe place.*]		
Maintenance	[Describe*here how the physical maintenance of the hardware is handled and indicate whether it has been contracted.* *Indicate whether remote maintenance of apps is allowed and how.* *Specify whether the defective equipment is specifically managed.*]		
Security of IT channels (networks)	[*Indicate here the type of network on which the processing is carried out (isolated, private or Internet).*		

General security checks relating to the system in which the processing is carried out	Implementation or justification why not	Is it acceptable/can it be improved?	Corrective checks
	Specify which firewall system, intrusion detection systems or other active or passive devices are in charge of ensuring network security.]		
Monitoring	[*Indicate here whether real-time monitoring of the local loop is implemented and by what means.* *Indicate whether and by what means hardware and software configurations are monitored.*]		
Physical access control	[Indicate*here how physical access control is carried out with regard to the premises hosting the treatment (zoning, escort of visitors, use of passes, closed doors and so on).* *Indicate whether burglary alert procedures are in place.*]		
Hardware security	[Indicate *here the physical security controls of the servers and workstations belonging to customers (secure storage, security cables, confidentiality filters, secure deletion before demolition, etc.).]*		

Avoid sources of risk	[Indicate*here whether the planting area is prone to environmental disasters (flood zone, proximity to chemical industries, seismic or volcanic zone, etc.).* *Specify if dangerous products are*		

General security checks relating to the system in which the processing is carried out	Implementation or justification why not	Is it acceptable/can it be improved?	Corrective checks
Protection against non-human sources of risk	[Describe*here the means of preventing, detecting and combating fires.* *Where appropriate, indicate the means to prevent water damage.* *In addition, the means of monitoring and rescue of the power supply shall be specified.]*		

Description and evaluation of organisational controls (governance)

Organisational controls (governance)	Implementation or justification why not	Is it acceptable/can it be improved?	Corrective checks
Organisation	[*Indicate whether data protection roles and responsibilities are defined.* *Specify whether a person is responsible for enforcing privacy laws and regulations.* *Specify whether there is a monitoring committee (or equivalent) responsible for the guidance and follow-up of privacy-related actions.]*		
Policy (rules management)	[Indicate*whether there is an IT card (or equivalent) on data protection and the proper use of IT resources.]*		
Risk management	[Indicate*here whether the privacy risks posed by the new data processing operations subjects are assessed, whether or not it is systematic and, if so, by what method.* *Specify whether an organization level* *The mapping of privacy risks is established.*]		
Project management	[Indicate*here if device tests are performed on non-real/anonymous data.]*		

Incident and data breach management	[Indicate*here whether cyber incidents are subject to a documented and tested management procedure.]*		
Personnel management	[*Indicate here which awareness checks are carried out with* *As for a new recruit.* *Indicate which controls are*		

Organisational controls (governance)	Implementation or justification why not	Is it acceptable/can it be improved?	Corrective checks
	carried out when persons who have had access to the data leave their jobs.]		
Relations with third parties	[*Indicate here, for transformers requiring access to data, security controls and the modalities of such access.]*		
Supervision	[Indicate*here whether the effectiveness and adequacy of privacy controls are being monitored.*]		

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						

Risk assessment

Risks	Is it acceptable/can it be improved?	Corrective checks	Residual severity	Residual probability
Illegitimate access to data	[The *evaluator must determine whether the existing or planned controls (already carried out) reduce this risk sufficiently to be considered acceptable.*]	[Where*appropriate, indicate here any additional checks that may be necessary.*]		
Unwanted modification of data	[The *evaluator must determine whether the existing or planned controls (already carried out) reduce this risk sufficiently to be considered acceptable.*]	[Where *appropriate, indicate here any additional checks that may be necessary.*]		
Disappearance of data	[The *evaluator must determine whether the existing or planned controls (already carried out) reduce this risk sufficiently to be considered acceptable.*]	[Where *appropriate, indicate here any additional checks that may be necessary.*]		