Co-funded by the European Union

Smart Survey Implementation

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

Work package 5

Legal

Deliverable 5.1: Review stage report

Version 0.1, 2023-10-16

Prepared by:

Cecilia Colasanti (Istat, Italy)
Claudia De Vitiis (Istat, Italy)
Monica Perez (Istat, Italy)

Work package Leader:

Cecilia Colasanti (Istat, Italy)
e-mail address : cecolasa@istat.it
telephone : +390646732228

Disclaimer: Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Eurostat. Neither the European Union nor the granting authority can be held responsible for them.

Index

1. Introduction

This document is a first intermediate result of work package 5 of the SSI project.

The main goals of WP5 – at the end of the project – are:

1. Identify legal requirements specific to shared smart micro-services
2. Determine what may be considered informed consent for different smart features
3. Determine decision rules in making trade-offs between in-house processing and in-device processing, i.e. data minimization/privacy by design versus quality control, including role of Privacy-Enhancing-Techniques (PET)
4. Determine guidelines for third-party-involvement
5. Make updating of DPIA for new smart features more efficient
6. Harmonize ESS-wide legal perceptions of NSI's
7. Confront legal requirements with ethical/NSI-policy requirements

Aim of this document is to share a useful template of Data Protection Impact Analysis (DPIA) and a guide to fill in it, taking into consideration the particular elements that characterize the smart statistics.

2. DPIA - Template and user guide

This template and related user guide represents a useful document for statisticians to evaluate risks connected with statistic processes and data processing.

Based on the EDPS guidelines[1] , the first section is dedicated to the statistical process description and the second section to the balancing the objectives of the statistical work with the principles of the General Data Protection Regulation (art. 5).

The approach is risk based, following the instructions released by ENISA[2].

[1] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0 Adopted on 20 October 2020

[2] https://www.enisa.europa.eu/risk-level-tool/risk

Appendix 1: DPIA - Template and user guide

Data Protection Impact Assessment
(art. 35 GDPR)

Project name:

Involved NSI:

[PART I IS FILLED IN BY STATISTICIANS]

PART I *– Information on data processing*

1. ***Controller*** *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. Controllers make decisions about processing activities.*
   [PUT THE NAME OF NIS THAT PERFORMS THE BUSINESS CASE - the final document will be submitted to the Data Protection Officer of each NIS for his opinion and we have to decide together if sending the document to the Data Protection Authority of the member state of controller]

2. ***Co-controller*** *Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers*
   PUT THE NAME OF OTHER NIS THAT PERFORM THE BUSINESS CASE WITH CONTROLLER [we evaluate if the final document will be submitted also to the Data Protection Authority of the member state of co-controller]

3. ***Processor*** *means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the* **contract or other legal act** *between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations*
   IF THERE IS A SUPPILER (OR MORE) IT IS NECESSARY TO ATTACH THE CONTRACT OR OTHER LEGAL ACT

4. ***Data processing description***

Describe, in a clear and simple way, the nature, scope, context and purposes of statistical project and the related data processing, the relationship among data and information, also using flow chart, regardless privacy principles.

5. Data sources and variables

Describe input and output list of data sources and variables needed by the project

6. Recipients or categories of recipients of the personal data

Recipients means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not

Example of categories of recipients are: students, teachers, journalist, or everyone is involved in the business case

7. Data communication and data dissemination

How data are disseminated (no disaggregated variable) Attach a methodological note with risk of re-identification

8. Start and end of data processing

Insert when (date or under which conditions) the data processing starts.

Insert when (date or under which conditions) the data processing ends.

[DPO AND/OR LEGAL DEPARTMENT HELP STATISTICIANS, ICT DEPARTMENT, SUPPLIER TO FILL IN PART II, ON THE BASE OF PART I – SPECIAL ATTENTION IS DEDICATED TO MINIMIZATION AND INTEGRITY AND CONFIDENTIALITY PRINCIPLES]

PART II *– GDPR Compliance on Article 25 Data Protection by Design and by Default based on Guidelines[1] 4/2019*

Transparency

The controller must be clear and open with the data subject about how they will collect, use and share personal data. Transparency is about enabling data subjects to understand, and if necessary, make use of their rights in Articles 15 to 22. The principle is embedded in Articles 12, 13, 14 and 34. Measures and safeguards put in place to support the principle of transparency should also support the implementation of these Articles.

Key design and default elements

Clarity	Information shall be in clear and plain language, concise and intelligible
Semantics	Communication should have a clear meaning to the audience in question
Accessibility	Information shall be easily accessible for the data

[1] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

subject.

Contextual — Information should be provided at the relevant time and in the appropriate form

Relevance — Information should be relevant and applicable to the specific data subject.

Universal design — Information shall be accessible to all data subjects, include use of machine

Comprehensible — Data subjects should have a fair understanding of what they can expect with

Multi-channel — Information should be provided in different channels and media, not only the

Layered — The information should be layered in a manner that resolves the tension between

Lawfulness

The controller must identify a valid legal basis for the processing of personal data. Measures and safeguards should support the requirement to make sure that the whole processing lifecycle is in line with the relevant legal grounds of processing.

Key design and default elements

Relevance — The correct legal basis shall be applied to the processing

Differentiation — The legal basis used for each processing activity shall be differentiated

Specified purpose — The appropriate legal basis must be clearly connected to the specific purpose of processing

Necessity — Processing must be necessary and unconditional for the purpose to be lawful

Autonomy — The data subject should be granted the highest degree of autonomy as possible with respect to control over personal data within the frames of the legal basis

Gaining consent — Consent must be freely given, specific, informed and unambiguous.28 Particular consideration should be given to the capacity of children and young people to provide informed consent

Consent withdrawal

Where consent is the legal basis, the processing should facilitate withdrawal of consent. Withdrawal shall be as easy as giving consent. If not, then the consent mechanism of the controller does not comply with the GDPR.29

Balancing of interests

Where legitimate interests is the legal basis, the controller must carry out a weighted balancing of interest, giving particular consideration to the power imbalance, specifically children under the age of 18 and other vulnerable groups. There shall be measures and safeguards to mitigate the negative impact on the data subjects

Predetermination

The legal basis shall be established before the processing takes place

Cessation

If the legal basis ceases to apply, the processing shall cease accordingly

Adjust

If there is a valid change of legal basis for the processing, the actual processing must be adjusted in accordance with the new legal basis.

Allocation of responsibility

Whenever joint controllership is envisaged, the parties must apportion in a clear and transparent way their respective responsibilities vis-à-vis the data subject, and design the measures of the processing in accordance with this allocation

Fairness

Fairness is an overarching principle which requires that personal data should not be processed in a way that is unjustifiably detrimental, unlawfully discriminatory, unexpected or misleading to the data 31 See Article 6(1)(b) GDPR. Adopted 18 subject. Measures and safeguards implementing the principle of fairness also support the rights and freedoms of data subjects, specifically the right to information (transparency), the right to intervene (access, erasure, data portability, rectify) and the right to limit the processing (right not to be subject to automated individual decision-making and non-discrimination of data subjects in such processes).

Key design and default elements

Autonomy

Data subjects should be granted the highest degree of autonomy possible to determine the use made of their personal data, as well as over the scope and conditions of that use or processing

Interaction Data subjects must be able to communicate and exercise their rights in respect of the personal data processed by the controller.

Expectation Processing should correspond with data subjects' reasonable expectations.

Non-discrimination The controller shall not unfairly discriminate against data subjects

Non-exploitation The controller should not exploit the needs or vulnerabilities of data subjects

Power balance Power balance should be a key objective of the controller-data subject relationship. Power imbalances should be avoided. When this is not possible, they should be recognised and accounted for with suitable countermeasures.

No risk transfer Controllers should not transfer the risks of the enterprise to the data subjects

No deception Data processing information and options should be provided in an objective and neutral way, avoiding any deceptive or manipulative language or design.

Respect rights The controller must respect the fundamental rights of data subjects and implement appropriate measures and safeguards and not impinge on those rights unless expressly justified by law

Ethical The controller should see the processing's wider impact on individuals' rights and dignity

Truthful The controller must make available information about how they process personal data, they should act as they declare they will and not mislead the data subjects

Human intervention The controller must incorporate qualified human intervention that is capable of uncovering biases that machines may create in accordance with the right to not be subject to automated individual decision making in Article 22.32

Fair algorithms Regularly assess whether algorithms are functioning in line with the purposes and adjust the algorithms to mitigate uncovered biases and ensure fairness in the processing. Data subjects should be informed about the functioning of the processing of personal data based on algorithms that analyse or make predictions about them, such as work performance, economic situation, health, personal preferences, reliability or behaviour, location or movements

Purpose Limitation

The controller must collect data for specified, explicit, and legitimate purposes, and not further process the data in a manner that is incompatible with the purposes for which they were collected. The design of the processing should therefore be shaped by what is necessary to achieve the purposes. If any further processing is to take place, the controller must first make sure that this processing has purposes compatible with the original ones and design such processing accordingly. Whether a new purpose is compatible or not, shall be assessed according to the criteria in Article 6.

<u>Key design and default elements</u>

Predetermination	The legitimate purposes shall be determined before the design of the processing
Specificity	The purposes shall be specified and explicit as to why personal data is being processed
Purpose orientation	The purpose of processing should guide the design of the processing and set processing boundaries
Necessity	The purpose determines what personal data is necessary for the processing
Compatibility	Any new purpose must be compatible with the original purpose for which the data was collected and guide relevant changes in design
Limit further processing	The controller should not connect datasets or perform any further processing for new incompatible purposes
Limitations of reuse	The controller should use technical measures, including hashing and encryption, to limit the possibility of repurposing personal data. The controller should also have organisational measures, such as policies and contractual obligations, which limit reuse of personal data.
Review	The controller should regularly review whether the processing is necessary for the purposes for which the data was collected and test the design against purpose limitation

Data Protection Impact Assessment
(art. 35 GDPR)

Data Minimization
Only personal data that is adequate, relevant and limited to what is necessary for the purpose shall be processed. As a result, the controller has to predetermine which features and parameters of processing systems and their supporting functions are permissible. Data minimisation substantiates and operationalises the principle of necessity. In the further processing, the controller should periodically consider whether processed personal data is still adequate, relevant and necessary, or if the data shall be deleted or anonymized.
Controllers should first of all determine whether they even need to process personal data for their relevant purposes. The controller should verify whether the relevant purposes can be achieved by processing less personal data, or having less detailed or aggregated personal data or without having to process personal data at all. Such verification should take place before any processing takes place, but could also be carried out at any point during the processing lifecycle. This is also consistent with Article 11. Minimising can also refer to the degree of identification. If the purpose of the processing does not require the final set of data to refer to an identified or identifiable individual (such as in statistics), but the initial processing does (e.g. before data aggregation), then the controller shall delete or anonymize personal data as soon as identification is no longer needed. Or, if continued identification is needed for other processing activities, personal data should be pseudonymized to mitigate risks for the data subjects' rights

<u>Key design and default elements</u>

Data avoidance	Avoid processing personal data altogether when this is possible for the relevant purpose
Limitation	Limit the amount of personal data collected to what is necessary for the purpose
Access limitation	Shape the data processing in a way that a minimal number of people need access to personal data to perform their duties, and limit access accordingly.
Relevance	Personal data should be relevant to the processing in question, and the controller should be able to demonstrate this relevance
Necessity	Each personal data category shall be necessary for the specified purposes and should only be processed if it is not possible to fulfil the purpose by other means
Aggregation	Use aggregated data when possible
Pseudonymization	Pseudonymize personal data as soon as it is no

longer necessary to have directly identifiable personal data, and store identification keys separately

Anonymization and deletion Where personal data is not, or no longer necessary for the purpose, personal data shall be anonymized or deleted

Data flow The data flow should be made efficient enough to not create more copies than necessary

" State of the art” The controller should apply up to date and appropriate technologies for data avoidance and minimisation

Accuracy

Personal data shall be accurate and kept up to date, and every reasonable step shall be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. The requirements should be seen in relation to the risks and consequences of the concrete use of data.
Inaccurate personal data could be a risk to the data subjects’ rights and freedoms, for example when leading to a faulty diagnosis or wrongful treatment of a health protocol, or an incorrect image of a person can lead to decisions being made on the wrong basis either manually, using automated decision-making, or through artificial intelligence.

<u>Key design and default elements</u>

Data source Sources of personal data should be reliable in terms of data accuracy

Degree of accuracy Each personal data element should be as accurate as necessary for the specified purposes

Measurably accurate Reduce the number of false positives/negatives, for example biases in automated decisions and artificial intelligence

Verification Depending on the nature of the data, in relation to how often it may change, the controller should verify the correctness of personal data with the data subject before and at different stages of the processing (e.g. to age requirements)

Erasure/rectification The controller shall erase or rectify inaccurate data without delay. The
controller shall in particular facilitate this where

the data subjects are or were children and later want to remove such personal data

Error propagation avoidance Controllers should mitigate the effect of an accumulated error in the processing chain

Access Data subjects should be given information about and effective access to personal data in accordance with the GDPR articles 12 to 15 in order to control accuracy and rectify as needed.

Continued accuracy Personal data should be accurate at all stages of the processing, tests of
accuracy should be carried out at critical steps.

Up to date Personal data shall be updated if necessary for the purpose

Data design Use of technological and organisational design features to decrease inaccuracy, for example present concise predetermined choices instead of free text fields

Storage limitation

The controller must ensure that personal data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. It is vital that the controller knows exactly what personal data the company processes and why. The purpose of the processing shall be the main criterion to decide in how long personal data shall be stored. Measures and safeguards that implement the principle of storage limitation shall complement the rights and freedoms of the data subjects, specifically, the right to erasure and the right to object.

Key design and default elements

Deletion and anonymization The controller should have clear internal procedures and functionalities for deletion and/or anonymization

Effectiveness of anonymization/deletion The controller shall make sure that it is not possible to re-identify anonymized data or recover deleted data, and should test whether this is possible

Automation Deletion of certain personal data should be automated

Storage criteria

The controller shall determine what data and length of storage is necessary for the purpose

Justification

The controller shall be able to justify why the period of storage is necessary for the purpose and the personal data in question, and be able to disclose the rationale behind, and legal grounds for the retention period

Enforcement of retention policies

The controller should enforce internal retention policies and conduct tests of whether the organization practices its policies

Data flow

Controllers should beware of the flow of personal data, and the storage of any copies thereof, and seek to limit their "temporary" storage.

Backups/logs

Controllers shall determine what personal data and length of storage is necessary for back-ups and logs

Integrity and confidentiality

The principle of integrity and confidentiality includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. The security of personal data requires appropriate measures designed to prevent and manage data breach incidents; to guarantee the proper execution of data processing tasks, and compliance with the other principles; and to facilitate the effective exercise of individuals' rights. Recital 78 states that one of the DPbDD measures could consist of enabling the controller to "create and improve security features". Along with other DPbDD measures, Recital 78 suggests a responsibility on the controllers to continually assess whether it is using the appropriate means of processing at all times and to assess whether the chosen measures actually counter the existing vulnerabilities. Furthermore, controllers should conduct regular reviews of the information security measures that surround and protect personal data, and the procedure for handling data breaches

Key design and default elements

Information security management system (ISMS)

Have an operative means of managing policies and procedures for information security

Security by design

Consider security requirements as early as possible in the system design and development and continuously integrate and perform relevant tests

Risk analysis

Assess the risks against the security of personal data by considering the impact on individuals' rights and counter identified risks. For use in risk assessment; develop and maintain a comprehensive, systematic and realistic "threat modelling" and an attack surface analysis of the designed software to reduce attack vectors and opportunities to exploit weak points and vulnerabilities

Maintenance

Regular review and test software, hardware, systems and services, etc. to uncover vulnerabilities of the systems supporting the processing

Access control management

Only the authorized personnel who need to should have access to the personal data necessary for their processing tasks, and the controller should differentiate between access privileges of authorized personnel.

- Access limitation (agents) – Shape the data processing in a way that a minimal number of people need access to personal data to perform their duties, and limit access accordingly.
- Access limitation (content) – In the context of each processing operation, limit access to only those attributes per data set that are needed to perform that operation. Moreover, limit access to data pertaining to those data subjects who are in the remit of the respective employee
- Access segregation – Shape the data processing in a way that no individual needs comprehensive access to all data collected about a data subject, much less all personal data of a particular category of data subjects.

Secure transfers

Transfers shall be secured against unauthorized and accidental access and changes

Secure storage

Data storage shall be secure from unauthorized access and changes. There should be procedures to assess the risk of centralized or decentralized storage, and what categories of personal data this applies to. Some data may need additional security measures than others or isolation from others

Pseudonymization

Personal data and back-ups/logs should be pseudonymized as a security measure to minimise risks of potential data breaches, for example using hashing or encryption

Backups/ logs

Keep back-ups and logs to the extent necessary for information security, use audit trails and event monitoring as a routine security control. These shall be protected from unauthorised and accidental access and change and reviewed regularly and incidents should be handled promptly

Disaster recovery/ business continuity

Address information system disaster recovery and business continuity requirements to restore the availability of personal data following up major incidents.

Protection according to risk

All categories of personal data should be protected with measures adequate with respect to the risk of a security breach. Data presenting special risks should, when possible, be kept separated from the rest of the personal data

Security incident response management

Have in place routines, procedures and resources to detect, contain, handle, report and learn from data breaches

Incident management

Controller should have processes in place to handle breaches and incidents, in order to make the processing system more robust. This includes notification procedures, such as management of notification (to the supervisory authority) and information (to data subjects).

PART III – *Risk analysis*

Fill in the excel based on the ENISA tool

https://www.enisa.europa.eu/risk-level-tool/risk

https://www.enisa.europa.eu/risk-level-tool/methodology

Istituto Nazionale di Statistica

Direzione Centrale per i rapporti esterni, le relazioni internazionali, l'ufficio stampa e il coordinamento del Sistan (DCRE)

Servizio Protezione dei dati personali, monitoraggio dei sistemi di sicurezza e rapporti con gli interessati (RPD)

Subject: Summary relating to the data processing carried out in the survey "New methods for collecting data in statistical surveys", preliminary experimentation on the use of data collection techniques (smartphone app for compiling the diary) for the implementation of the survey Time Use (IST-01858)

Aim of the statistical work is to know the opinions of the population regarding the new methods of data collection (apps, use of sensors and similar) and to investigate the willingness to use intelligent devices in official statistical surveys.

The survey, carried out in Italy, Holland and Slovenia, in addition to being foreseen in the current national statistical program[1], is carried out as part of the Smart Survey Implementation (SSI) project, to which grant no. 101119594 (2023-NL-SSI) is dedicated, financed by Eurostat, and of which Istat is a partner.

This work represents a great opportunity for methodological research on innovative techniques and tools to modernize data collection processes. In fact, even today the compilation of diaries in TimeUse survey is anchored to the use of paper questionnaires. This implies a high statistical burden on respondents, requiring a long time to complete.

The Data Protection Impact Analysis was carried on before starting the data processing and the whole documentation is available, on demand, in Istat (Istat prot. n. 2275622/23 del 17/10/2023).

[1] https://www.sistan.it/index.php?id=668