Tools4LEAs

A project of the European Anti-Cybercrime Technology Development Association (EACTDA)

EACTDA

D1.8 Ethical, legal, privacy, and social impact management Handbook

This project ~~that~~ has received funding from the European Union's ISF Police programme, under grant agreement no 101036219.

Version:	1.0	
Delivery date:	September 2021	
Dissemination level:	Public	
Status	FINAL	
Nature:	Report	
Main author(s):	Juan Arraiza	EACTDA
Contributor(s):	Sigute Stankeviciute	L3CE

DOCUMENT CONTROL

Version	Date	Author(s)	Change(s)
0.1	26/08/2021	Juan Arraiza (EACTDA)	TOC and initial text
0.2	27/08/2021	Juan Arraiza (EACTDA)	First version for all sections completed. Requested contributions from EACTDA members and key stakeholders.
0.3	29/09/2021	Juan Arraiza (EACTDA)	Updated with received minor corrections and fixes, and feedback from Sigute Stankeviciute (L3CE).
1.0	30/09/2021	Juan Arraiza (EACTDA)	Final version, ready to be submitted

TABLE OF CONTENTS

1. Introduction

1.1. Main objective of this document

The main objective of this document is to provide reference materials and guidelines to aid ensuring that the project is implemented in compliance with all ethical, privacy, and data protection principles and regulations.

This document focuses on the guidelines, procedures, and necessary templates support the following activities:

- Creation and update of a Data Management Plan.
- Preparation, execution, and reporting of a data protection impact assessment.
- Preparation, execution, and reporting of a social impact assessment.
- Preparation, execution, and reporting of an ethics assessment.

Also, to undertake these activities in a trustworthy and independent way, it is worth noting that the Tools4LEAs project has allocated some budget to hire external experts. This document will serve as a starting point for them to carry out their work, but it is not intended to constrain it.

1.2. Relation to other deliverables

This deliverable is closely related to the following deliverables:

- **D1.9 and D1.10 report on Ethical, legal, privacy, and social impact activities:** These two deliverables will report the progress and performance made on the activities related to social impact, ethical, legal, and privacy matters of the project. D1.10 will also report about the results of a Data Protection Impact Assessment, a Social Impact Assessment, and an Ethics Assessment.
- **All other Tools4LEAs deliverables:** all other project deliverables should take into account the considerations and policies presented in D1.8 with regard to data management and or compliance with social, ethical, legal and privacy laws and obligations.

1.3. Structure of the deliverable

Section 2 describes the process of creation and update of the Data Management Plan for the project.

Section 3 presents the process for the preparation, execution, and reporting of data protection impact assessments.

Section 4 presents the process for the preparation, execution, and reporting of a social impact assessment.

Section 5 presents the process for the preparation, execution, and reporting of an ethics assessment.

And, finally, section 6 summarises which is the goal and key aspects of this document, it acknowledges that there is still work to be done to improve the document, and it presents some of the areas of future work that have already been identified.

2. Data Management Plan

Good data management starts with the creation of a good Data Management Plan (DMP) which should describe the data management life cycle for the data to be collected, processed and/or generated by, in this case, the Tools4LEAs project.

This DMP is intended to be a living document in which information will most likely be made available on a finer level of granularity through updates as the implementation of the project progresses and when significant changes occur.

2.1. Data Summary

2.1.1. What is the purpose of the data collection/generation and its relation to the objectives of the project?

During the project, it will be necessary to collect/generate data for software development of artificial intelligence (AI)-based tools/components. This data will be used for training new AI models and/or for evaluating the tools/components developed.

Also, during the course of the project demonstration and evaluation events will be organized. During these events, information about the professional background and/or the expertise of the participants in the events might be required.

2.1.2. What types and formats of data will the project generate/collect?

For the most part of it, this information is not known yet, as it will depend on the scope of the new software tools/components that the project ends-up deciding to undertake, and as of September 2021 this information is not available yet. Deliverables D1.9 and D1.10, due months 12 and 24 respectively, will include this information.

The project will generate and collect administration data such as contact details of participants to the six-monthly demonstration and evaluation events or to other workshops or meetings, or data collected from expert and project participants via interviews, surveys, etc. It is not expected to collect large amounts of this type of administrative data.

2.1.3. Will you re-use any existing data and how?

Yes, publicly available scientific/research datasets[1] will be re-used as necessary during the course of the project. In most cases, this type of datasets will be used to evaluate the results of the new software tools/components developed during the project.

2.1.4. What is the origin of the data?

See response to sub-section 2.1.2.

[1] E.g., CIFAR-10 or Cityscapes for computer vision, Enron dataset or SMS Spam collection for natural language processing.

2.1.5. What is the expected size of the data?

See response to sub-section 2.1.2.

2.1.6. To whom might it be useful ('data utility')?

To the developers of the new tools and to the testers and end-users testing and evaluating those tools.

2.2. Making data findable

2.2.1. Are the data produced and/or used in the project discoverable with metadata, identifiable and locatable by means of a standard identification mechanism (e.g., persistent and unique identifiers such as Digital Object Identifiers)?

When possible, Digital Object Identifiers will be used/generated and published.

2.2.2. What naming conventions do you follow?

General Guidelines

- Include a text file, often called a readme, in your file directory that describes the naming conventions you are using. This information will be helpful for individuals who are new to the project.
- Use descriptive file names that are meaningful to you and your colleagues. This might include the project name, subject, or acronym.
- Keep file names relatively short (no more than 25 characters when possible).
- Include dates in your filename, which can help with sorting different versions of your file. Recommended format: yyyymmdd.
- Use a sequential numbering system to keep track of different versions or revisions to a file. For example, try with leading 0's. (rehab01 instead of rehab1)
- Use hyphens, underscores, or camelCase instead of spaces.

Things to Avoid

- Spaces within your files; not all software recognizes spaces within file names.
- Special characters in your file names such as: "/ \ : * ? " < > [ ] & $. These characters have specific meanings for various operating systems and could result in your files being deleted or misplaced.
- Long or wordy names that may not have meaning to you and other researchers on your team.

Recommended naming convention:

- *[project-name]_[date (if/when applicable)]_[filename]_[version].[filetype]*

Example:

- Tools4LEAs_20210827_D1.8_v0.2.docx

2.2.3. Will search keywords be provided that optimize possibilities for re-use?

Yes

2.2.4. Do you provide clear version numbers?

Yes. The convention will be as follows:

vx.y (e.g., v1.2)

"x" will be used for approved versions of the document/file.

"y" will be used for draft versions when "x" is "0" or for minor changes/updates if "x" is higher than "0".

2.2.5. What metadata will be created? In case metadata standards do not exist in your discipline, please outline what type of metadata will be created and how.

This will depend on the type of data. See response to sub-section 2.1.2.

2.3. Making data accessible

2.3.1. Which data produced and/or used in the project will be made openly available as the default?

Whenever possible (when there are no restrictions), the data will be made openly available. However, this will depend on the type of data. See response to sub-section 2.1.2.

2.3.2. How will the data be made accessible (e.g. by deposition in a repository)?

Data will be made accessible by deposition in a repository. When looking for a repository for data, firstly it will be checked whether there is a thematic/community database where the data could be archived. Irrespective of the repository chosen, it will be checked whether it is sustainable in the longer term, the data is stored in a safe way, the data will remain findable, accessible and re-usable. Also, it will be checked if the repository describes the data in a standard way and uses accepted metadata standards and that it allows the Tools4LEAs project to specify a license governing access and re-usability of the data.

Well-known repositories such as Zenodo, Github, or Open Science Framework will be the first ones to be considered for deposition of data.

2.3.3. What methods or software tools are needed to access the data?

This will depend on the repositories finally chosen to deposit the data, though simple and easy-to-access methods such as web browsers and/or ftp will be prioritized.

2.3.4. Is documentation about the software needed to access the data included?

This will depend on the repositories finally chosen to deposit the data.

2.3.5. Is it possible to include the relevant software (e.g. in open source code)?

This will depend on the Intellectual Property Rights of the software.

2.3.6. Where will the data and associated metadata, documentation and code be deposited?

Data and the associated metadata, documentation and code will be deposited at EACTDA's repository. Access to it will be restricted to authorised users only.

2.3.7. Have you explored appropriate arrangements with the identified repository?

Yes. The repository will be owned and managed by EACTDA.

2.3.8. If there are restrictions on use, how will access be provided?

EACTDA will determine the access levels restrictions and it will provide access to the data.

2.3.9. Is there a need for a data access committee?

Yes. EACTDA Secretariat, following the instructions of the End-User Advisory Board of the Toosl4LEAs project will determine the access rights to the repository and to the data stored in it.

2.3.10. Are there well described conditions for access (i.e. a machine readable license)?

Not yet, though this will be considered for future enhancements of EACTDA repository.

2.3.11. How will the identity of the person accessing the data be ascertained?

This has not been decided yet, though at minimum a user+password mechanisms will be implemented, and, if possible, a two factor authentication method yet to be decided will also be used.

2.4. Making data interoperable

2.4.1. Are the data produced in the project interoperable, that is allowing data exchange and re-use between researchers, institutions, organisations, countries, etc. (i.e. adhering to standards for formats, as much as possible compliant with available (open) software applications, and in particular facilitating re-combinations with different datasets from different origins)?

The Tools4LEAs project will observe OpenAIRE guidelines for online interoperability, including OpenAIRE Guidelines for Literature Repositories, OpenAIRE Guidelines for Data Archives, OpenAIRE Guidelines for CRIS Managers based on CERIF-XML. These guidelines can be found at: https://guidelines.openaire.eu/en/latest/.

Partners will also ensure that BLAZE data observes FAIR data principles under H2020 open-access policy:

http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oadatamgt_en.pdf

In order to ensure the interoperability, all datasets will use the same standards for data and metadata capture/creation.

As the project progresses and data is identified and collected, making it as interoperable as possible will be a primary objective. In specific, an effort will be done to ensure the use of data and metadata vocabularies, standards or methodology to follow to facilitate interoperability.

2.4.2. What data and metadata vocabularies, standards or methodologies will you follow to make your data interoperable?

At present, it has not been decided to use any data and metadata vocabularies, standards or methodologies specific to the security field.

However, initiatives such as the ontology developed in the scope of H2020 projects like MAGNETO or PREVISION, the Universal Message Format (UMF) promoted by Europol, and Cyber-investigation Analysis Standard Expression (CASE) standard are being monitored and considered for future use.

In a more general perspective the "DCAT application profile for European data portals" (DCAT-AP), developed in the framework of the EU ISA Programme will be used when/as appropriate. The European Data Portal is implementing the DCAT-AP as the common vocabulary for harmonising descriptions of datasets harvested from several data portals of 34 countries. The DCAT-AP specification is available at: https://joinup.ec.europa.eu/asset/dcat_application_profile/.

2.4.3. Will you be using standard vocabularies for all data types present in your data set, to allow inter-disciplinary interoperability?

Using standard vocabularies will be done as much as possible, but it cannot guarantee that it will be done for all data types, as it is still not known at present the details of all the data sets that will be used.

2.4.4. In case it is unavoidable that you use uncommon or generate project specific ontologies or vocabularies, will you provide mappings to more commonly used ontologies?

Yes.

2.5. Increase data reuse

2.5.1. How will the data be licensed to permit the widest re-use possible?

When no security, confidentiality, or IPR issues are expected, the data will be licensed unrestricted.

When restrictions apply, it will be considered whether it is possible to produce and license with no restrictions samples of aggregated data.

2.5.2. When will the data be made available for re-use?

No embargos are foreseen, so in principle data with no restrictions will be made available for re-use as soon as it is possible.

2.5.3. Are the data produced and/or used in the project useable by third parties, in particular after the end of the project?

Data will be made available to third parties in accordance to the licensing conditions described in 2.5.1.

2.5.4. How long is it intended that the data remains re-usable?

No time limit has been foreseen for making data re-usable, and the time that the data itself will remain re-usable will depend on the specific characteristics of each dataset, as some might expire sooner than others.

2.5.5. Are data quality assurance processes described?

Data quality assurance is the process of identification and elimination of any data anomalies via the processes of data profiling and cleansing.

Good data quality requires disciplined data governance, rigorous management of incoming data, accurate requirement gathering, thorough regression testing for change management and careful design of data pipelines, in addition to data quality control programs for the data delivered both externally and internally. For all quality problems, it is much easier and less costly to prevent the data issue from happening in the first place, rather than relying on defending systems and ad hoc fixes to deal with data quality problems.

The process to ensure data quality assurance in the project is described as follows:

1. Rigorous data profiling and control of incoming data.
2. Careful data pipeline design to avoid duplicate data.
3. Accurate gathering of data requirements.
4. Enforcement of data integrity.
5. Integration of data lineage traceability into the data pipelines.
6. Automated regression testing as part of change management.
7. Capable data quality control teams.

2.6. Data security

2.6.1. What provisions are in place for data security (including data recovery as well as secure storage and transfer of sensitive data)?

From a security perspective, sensitive data is data that must be protected against unwanted disclosure, regardless of it being personal sensitive data or any other type of data (e.g., confidential data or classified information). In this sense, access to sensitive data should be safeguarded. Protection of sensitive data may be required for legal or ethical reasons, for issues pertaining to personal privacy, or for proprietary considerations.

Examples of sensitive data are:

- ***Personal data***: identifiers such as names or identification numbers, physical, physiological, genetic, mental, economic, cultural or social characteristics, it also includes location data from GPS or mobile phones. Sensitive personal data according to GDPR is data that reveals racial or ethical origin, political opinions, religious or philosophical believes, trade union membership,

biometric data, health data and sex life data (art 9(1) of GDPR). This type of sensitive personal data requires special protection and therefore has special regulation for processing.

- ***Confidential data***: trade secrets, investigations, data protected by intellectual property rights Security: passwords, financial information, national safety, military information...
- ***Combination of different datasets*** that can be combined into sensitive or personal data.
- ***Biological data***: endangered (plant or animal) species, where their survival is dependent on the protection of their location data (biodiversity community.
- ***Personal and sensitive metadata***

It is important to take into account that, when handling and dealing with sensitive data, special attention must be given to collecting, processing, handling and storing data.

In the Tools4LEAs project, all the data identified as sensitive will be encrypted using PGP, and only those people with the need-to-access the data will be granted access during the period in which they have the aforementioned need-to-access the data.

2.6.2. Is the data safely stored in certified repositories for long term preservation and curation?

Yes. Depending on the nature of the dataset, it might be stored in different repositories.

The Tools4LEAs project will have its own tools (and data) repository, which will be used for data that is restricted to authorised people, normally for the data that has certain security, confidential, or IPR related restrictions.

For any other data that does not have restrictions, domain-specific or general-purpose repositories will be used, depending again on the nature of the data at hand.

2.7. Ethical aspects

2.7.1. Are there any ethical or legal issues that can have an impact on data sharing?

These can also be discussed in the context of the ethics review. If relevant, include references to ethics deliverables and ethics chapter in the Description of the Action (DoA).

2.7.2. Is informed consent for data sharing and long-term preservation included in questionnaires dealing with personal data?

Yes.

2.8. Other issues

2.8.1. Do you make use of other national/funder/sectorial/departmental procedures for data management? If yes, which ones?

No.

3. Data Protection Impact Assessments

To prepare and conduct data protection impact assessments (DPIA), the Tools4LEAs project will adapt to its specific needs the template provided by the Spanish Data Protection Agency2.

The table of contents of the aforementioned template is as follows:

2 https://www.aepd.es/sites/default/files/2020-03/modelo-informe-EIPD-AAPP-en.rtf

The DPIA template for the Tool4LEAs project can be found in "ANNEX I – Data Protection Impact Assessment template".

4. Social Impact Assessments

The International Association of Impact Assessment (IAIA)[3] defines Social Impact Assessments (SIA) as being "*the processes of analyzing, monitoring and managing the intended and unintended social consequences, both positive and negative, of planned interventions (policies, programs, plans, projects) and any social change processes invoked by those interventions*".

A robust social analysis and consultation process involving local communities should also inform decisions about local priorities and needs, and be considered in determining the overall concept and design of a project, not just analysing and managing consequences of a pre-determined project approach. The SIA process should be reflected in project decision-making at all stages of a project cycle, in order to maximize value and minimize the social cost of an intervention. The project includes a budget bucket to hire external independent experts who will conduct data protection, privacy, ethical, and social impact assessments. These assessments will take place on a six-monthly bases, coinciding with the demonstration and evaluation events that the project will organise.

A key task in an SIA process is to identify the distributional aspects of potential benefits and risks the project may cause or contribute to, and to ensure that any adverse impacts do not fall disproportionately on the poor or vulnerable.

To strengthen project quality, sustainability, and acceptance, the Tools4LEAs project will implement SIA processes as part of its normal practices, and therefore, the social analysis, stakeholder engagement, and updating of plans and management systems will be embedded as core elements throughout the project's lifetime.

4.1. Ten principles of Social Impact Assessment

While the field of SIA is evolving, there is broad agreement among practitioners and institutions on some key aspects and characteristics of SIA. These can be summarized in the following ten principles:

The SIA should promote:

1. Equal opportunity, inclusion, and sustainability in a project setting.
2. Local benefits, community development, and capacity.
3. Empowerment and social capital.

The SIA should:

4. Be a proactive and integral part of project planning and implementation, interconnected with economic, physical, environmental and other issues.
5. Address both risks and opportunities.
6. Be rigorous in its use of data, which may include quantitative as well as qualitative data.
7. Be widely applicable in different contexts and settings.
8. Build on local knowledge and participatory processes, and reflect diversity in culture and values.
9. Respect and promote human rights, transparency and accountability, and the rule of law.

The SIA should not:

[3] https://iaia.org/

10. Apply coercion or undue force.

4.2. The SIA process in the Tools4LEAs project

The SIA process in the Tools4LEAs project should be designed and carried out in such a way that it helps develop projects that provide benefits and opportunities for all, and ensures that adverse impacts do not disproportionately affect the poor and vulnerable. To do so, the SIA process in the Tools4LEAs project has used the International Principles for Social Impact Assessment[4] and the SIA guidelines of the Inter-American Development Bank[5] as the main references. The Societal Readiness Thinking Tool[6] will also be considered as a way to conduct the SIA process in the Tools4LEAs project.

The SIA process in the Tools4LEAs project will include the following activities:

1. **Identification of the legal and normative foundation.**
   - Focused on European and national/local levels.
   - Respecting relevant international treaties and agreements such as UN conventions including ILO labor conventions or human rights standards.
   - With an eye on in-force and coming EU and national/local strategies, policies, and regulations.

2. **Assessment of the social context.**
   - To be meaningful, the SIA needs to relate the existing social context to the proposed project, and analyse what aspects of the social context are relevant.
   - Of particular relevance and importance is the question of resilience and vulnerability, and risk of adverse impacts, as an adverse impact caused by a project will affect vulnerable people more than those with more resources and resilience.
   - Risk from a social perspective therefore depends not just on what happens, but on who it happens to.
   - The analysis and consultation conducted as part of the SIA should identify who among the affected population is particularly vulnerable to adverse impacts.
   - The project should adopt differentiated measures so that adverse impacts do not fall disproportionately on the disadvantaged or vulnerable.
   - Assessing the social context means understanding how individuals and groups perceive themselves and each other, how they relate to each other, and what characteristics of these groups may be relevant in a project context.
   - Understanding the levels and types of opportunities and risk as they apply to different groups of stakeholders.

[4] https://www.iaia.org/uploads/pdf/IAIA-SIA-International-Principles.pdf

[5] https://publications.iadb.org/publications/english/document/Social_Impact_Assessment_Integrating_Social_Issues_in_Development_Projects.pdf

[6] https://www.thinkingtool.eu/

- Defining local[7] needs and priorities, which may determine the overall project concept and approach.
- The social context also includes organizational structures, existing conflicts or tensions, and governance structures such as representativeness and responsiveness of government institutions and services.
- Understanding legacy issues and past conflict or discrimination, previous experiences from government interventions, private sector activities, or quality of services may determine how supportive and engaged a group is likely to be in relation to a proposed project.
- Relationships among people are to a large part based on social identities such as economic class, gender, ethnicity, age, sexual orientation, disability, or other factors.
- Some social categories are changeable (e.g., education, occupation, or political ideology), and others are more difficult (e.g., age, ethnicity and sex) for individuals or groups to change; the SIA should take into account that the combination of identities is likely to have different implications than each of these factors seen in isolation.
- Individuals fall into several social categories that interrelate and affect each other.

3. **Conducting stakeholder analysis and meaningful engagement.**
   - There are four key stakeholder groups: (1) project beneficiaries, who are positively affected by the project; (2) groups adversely affected; (3) groups favoring the project who can affect project outcomes; and (4) groups opposed to the project who can also affect project outcomes.
   - Meaningful consultation with project stakeholders captures the views and perceptions of people who may be affected or have an interest in a development project, and provides a means to take their views into account as inputs to improved project design and implementation, thereby avoiding or reducing adverse impacts, and enhancing benefits.
   - It also enables people to understand their rights and responsibilities in relation to a project.
   - Also, greater transparency and involvement of stakeholders enhances trust, project acceptance, and local ownership, which are key to project sustainability and development outcomes.
   - The stakeholder consultation process should be ongoing and iterative throughout the project cycle, starting as early as possible.
   - Different categories of stakeholders should be represented and involved, including individuals and groups, as well as formal and informal local institutions.
   - The process should be transparent and based on factual information, including about the scope of consultation and ability of stakeholders to influence project decisions.
   - The process should be equitable and non-discriminatory, and ensure that poorer or more vulnerable parts of the affected stakeholders are given a voice.
   - Stakeholders should have prior information about relevant aspects of the project, in a language, format, and manner that is appropriate for them. Different approaches will be appropriate for different groups and in different contexts.
   - Consultation events and other forums or means of engaging with stakeholders should be respectful and free of coercion. Stakeholders who express concerns or criticism against the project or authorities should be protected from retaliation.

[7] Determining what "local" means in the context of the Tools4LEAs project is not trivial; for the time being we will refer to the societies of all European Union member states.

- Confidentiality of information and stakeholders should be ensured where appropriate.
- The process should be systematically documented, and relevant aspects of it should be disclosed publicly as long as no sensitive information is disclosed.

4. **Identification of benefits and opportunities.**
   - Opportunities for employment, or provision of goods and services to project beneficiaries.
   - Training and capacity building.
   - Involving communities actively in defining priorities through meaningful consultations, and participating actively in project planning and implementation, contributes to well targeted and more sustainable development with local ownership.

5. **Identification of risks.**
   - 'Impact' is part of the definition of risk, as risks refer to possible future and negative impacts.
   - Projects should ensure that any potential or actual adverse impacts are identified.
   - Adverse social impacts originated by the project should be avoided or reduced, and mitigated in different ways when they are unavoidable.
   - The effort involved in the SIA process should be proportionate to the expected level of risk in the project.
   - Risk levels are usually categorized as high, substantial, moderate, or low.
   - Once identified, the probability of occurrence or likelihood of the risk has to be determined.
   - Examples of social risks include labor issues, human rights violations, corruption by company officials, or malfunction of public services (this latter one probably being the most relevant one in the case of the Tools4LEAs project).

6. **Determining indicators, baselines, and data collection methodology.**
   - Any project should be able to answer some basic questions as part of a completion assessment: Are affected people better or worse off than before the project? Can the changes be attributed to the project, or are there other contributing factors? If there are adverse impacts from the project, have the mitigation mechanisms adequately compensated for such impacts, so that people at the end of the project have not experienced a net loss in their assets, livelihoods, or well-being?
   - Baseline data are needed to make comparisons and evaluations about project results and impacts.
   - The baseline data and benchmarking should be established during project preparation or, at least, before the project has an impact (positive or negative).
   - Baseline data should provide the basis for decisions about project location, design, operation, and mitigation measures. Throughout the project's lifetime, additional data should be collected through the project's monitoring system and other means. A discussion should be included about the accuracy, reliability, and sources of the data, any existing uncertainties or data gaps, and proposed steps to complete necessary data collection.
   - The data should be disaggregated by relevant social groups.
   - Both adversely affected people and project beneficiaries should be disaggregated by gender and other relevant social identities, and monitoring indicators should track prevention and mitigation measures reflecting this disaggregation.
   - The unit of analysis and entitlement (individuals, groups) for support will vary depending on the context.

- The validity and reliability of survey data and indicators selected for the baseline and subsequent studies can be greatly improved through verification with local stakeholders, who may also inform data collection methods such as a survey design by helping to identify important issues that are not apparent to outsiders.
- Developing indicators should be done in a participatory manner, to ensure that the analysis and future monitoring and evaluation capture variables and factors that are meaningful to local stakeholders (note: including also people's perceptions, not only objective data).
- Once baseline data has been obtained, it is necessary to establish benchmarks and target values (comparator data and what the project expects to achieve).
- The indicators used should be objectively verifiable to the extent possible, and may be based on both quantitative and qualitative data.

7. Reflecting social issues in project design and implementation.

- Risks must be managed, and this is done through applying a logical sequence of steps, referred to as a mitigation hierarchy.
  1. Identify and anticipate risks of potential adverse impacts, through analysis and consultation (discussed in previous sections)
  2. Avoid potential adverse impacts, applying an alternatives analysis including a no-project scenario.
  3. Minimize or reduce the impacts.
  4. Restore or rehabilitate where possible.
  5. Compensate or offset residual impacts.

8. Producing and disclosing reports and plans.

- The SIA process implemented in the project needs to be documented, including the analysis and consultations undertaken, and of the various action plans where relevant.
- In the Tools4LEAs project, deliverables "D1.9 - D1.10 report on Ethical, legal, privacy, and social impact activities" will report the work done in relation to the project's SIA process.

9. Embedding social issues within the project management system.

- The project should have a clearly stated policy or statement of commitment, with values, principles, objectives and goals that govern social performance.
- The project should also have an organizational structure to implement environmental and social commitments.
- The project should have a SIA process implementation plan. In the Tools4LEAs project, this deliverable (D1.8) is the plan.
- The project should have mechanisms for ongoing stakeholder engagement and feedback.
- The project should have mechanisms for monitoring, review, supervision, and evaluation.

10. Monitoring, adaptative management, and evaluation or results.

- A social impact management process can reduce but not eliminate risk. An essential measure of performance is therefore how efficiently and effectively a project responds to unforeseen circumstances. This is done through adaptive management, whereby a project establishes a flexible system for learning and adapting.

- An adaptive management approach requires systematic monitoring of the project's environmental and social performance and results, and ongoing consultations with key stakeholder groups.
- The indicators used for the monitoring should be based on the project's baseline data.
- Independent, third-party expert s may also be part of a project's monitoring system. This is the case of the Tools4LEAs project.

A Social Impact Assessment template that can be found in "ANNEX III – Social Impact Assessment template" has been produced to facilitate SIA in the Tools4LEAs project.

5. Ethics Assessments

The Tools4LEAs project will follow these ethic principles:

1. **Respect for autonomy**: duty to respect individuals' right of self-governance.
2. **Nonmaleficence**: duty to avoid causing harm and to minimize harm to individuals.
3. **Beneficence**: duty to maximize benefits and to enhance individual's well-being.
4. **Justice**: duty to treat individuals fairly and equitably.

In addition, the project commits to comply also with the following other principles:

- **Accountability & responsibility**: an ethical concept that refers to the fact that individuals and groups have morally based obligations and duties to others and to larger ethical and moral codes, standards and traditions.
- **Transparency**: an ethical concept that refers to an attribute of individual or corporate culture that's revealed through the behaviors of the individuals, in the case of an organization the behaviors of its leaders, employees, and stakeholders.
- **Honesty**: an ethical concept that is a component of moral character that connotes positive and virtuous attributes, such as integrity, truthfulness, and openness — including clarity of conduct, along with the absence of lying, cheating, theft, etc. Honesty also involves being reliable, trustworthy, loyal, fair, and sincere.
- **Fairness**: an ethical concept that is concerned with actions, processes, and consequences, that are morally right honorable, and equitable. In essence, the virtue of fairness establishes moral standards for decisions that affect others. Fair decisions are made in an appropriate manner based on appropriate criteria.
- **Non-discrimination**: an ethical concept that requires the equal treatment of an individual or group irrespective of their particular characteristics, and is used to assess apparently neutral criteria that may produce effects which systematically disadvantage persons possessing those characteristics.
- **Respect for human dignity, human rights & justice**: an ethical concept that refers to the inherent and inalienable value of every human being which cannot be destroyed, taken away or measured. It is not dependent or conditional on anything.

An ethics assessment template that can be found in "ANNEX IV – Ethics Assessment template" has been produced to facilitate ethic assessments.

6. Summary

6.1. Conclusion

In this document we have introduced the concepts of Data Management, Social Impact Assessment, and Ethics assessment. For each of these concepts, implementation guidelines and materials (mainly templates) have been presented.

6.2. Evaluation

The work presented in this document is considered to be sufficient to launch the SELP management processes of the Tools4LEAs project. However, the SELP management process, and therefore this handbook, will be updated during the lifetime of the project to adapt to the new needs.

6.3. Future work

Deliverables D1.9 and D1.10 will report the work done in relation to SELP matters, including the changes done to this deliverable (D1.8).

ANNEX I – Data Protection Impact Assessment template

I. EXECUTIVE SUMMARY

This summary must include, in a condensed manner, the most significant aspects of the chapters developed in the document.

It will contain the identification of the GDPR data controller, the department in charge for the processing operations, other departments involved in some of the phases of processing, data processors and sub-processors and intended data transfers.

At the same time, it will include a brief description of processing, its purpose, the main categories of data and the planned implementation.

It will also highlight the risk factors that require the DPIA and, in the event that the DPIA is not mandatory, a statement about why the data controller decides to carry out the DPIA.

Finally, it will include a brief description of the DPIA and the methodology used, the extension and limits of the DPIA, the main privacy risks identified, the benefits of processing, the management solutions and techniques planned, the cost-benefit analysis and the conclusions reached regarding the residual risk and, in particular, whether it is necessary or not to consult the DPA in advance (prior consultation).

II. TABLE OF CONTENTS

Include here the table of contents of the DPIA to be conducted

III. PURPOSE OF THE PROCESSING OPERATION

Date of preparation of the DPIA

Date, time and identification of the team leader that carries out the DPIA.

Version or review of the DPIA.

History of changes and modification, in general any element that can demonstrate the monitoring carried out by the processor

Name and Description of Processor

Internal name given to the processing operation, name used in the inventory of processing activities, and, if possible, the identification of the version of the processing operation indicating the log of changes and modifications made to the process, if any, in each of the phases of same.

A brief description of the processing operation, including the information established in (Article 30 GDPR) regarding the inventory of processing activities accessible by electronic means and the Records of Processing Activities themselves.

Categories of Data

It shall include a brief introductory description of the categories of data processed, in particular, regarding with the special categories of personal data, including the operations carried out on these in each of the phases into which the processing is decomposed.

Identification of the Data Controller as per GDPR

Identification of the Data Controller entity as per the GDPR and, if applicable, joint controllers

Identification of a Point of Contact (POC) with the Controller/Joint Controller entity (if applicable DPO) and each of the controllers or POC in each of the management units or functional units involved in processing. In Public Administrations, the position of Data Protection Officer shall be compulsory.

Identification of the units or units responsible for managing the processing within the controller organisation.

Identification of third parties involved in processing

This section will be completed based on how the implementation of processing is planned and the form and extension of contractual relations or any other binding legal instrument (collective agreements, protocols, instructions, etc.).

Identification of the entities that fulfil the role of Processors/Sub-processors as per GDPR.

Identification of POC in the Processor/Sub-processor entity (if applicable, DPO).

Internal context of the processing operation in the organisation

Brief description of the structure of the organisation, functions and competencies. Policies, adapted standards, organisational maturity objectives and the culture of the organisation in general.

Indicate some of the characteristics of the organisation such as, for example, the number of people involved in the processing operation, their profiles, roles and possible segregation of functions over the course of the life cycle of the processing operation.

Include the characteristics of the premises which may affect the data collection or processing operations, such as open rooms for citizen services, workplaces where screens, telephones, etc. are shared.

Identification of all the processes of the organisation that may be related to or affected by the processing operation in relation to the processes map.

Possible relationships with other processing activities of the organisation itself and elements that could be shared, for example, phases of other data processing that are common to the processing under analysis.

Context of the systems proposed for the implementation of processing and the detail of the technologies used.

External context of the organisation and the processing operation

This section will include a description of the environment in which the entity carries out processing, which can be understood as the social and cultural, political, legal, regulatory, financial and technological contexts, natural or competitive, at international, national, regional or local level.

In particular, the interaction of the processing operation with other processes external to the organisation with the data subjects.

IV. LAWFULNESS OF PROCESSING AND REGULATORY COMPLIANCE

This chapter looks at the legal basis and, where applicable, legislation and/or enabling circumstances.

One must be conscious that regulatory compliance does not form part of the analysis of risks but compliance with principles and rights is mandatory.

The absence of a legal basis for processing or the existence of any doubts regarding the legal basis cannot be substituted with the adoption risk management measures for the fundamental rights and freedoms of citizens.

In no case, the assessment for the adoption of a legal basis is the purpose of this document.

To complete this section, consult the "Regulatory Compliance List" published by the AEPD (in Spanish) at:

https://www.aepd.es/media/guias/guia-listado-de-cumplimiento-del-rgpd.pdf

V. DPIA METHODOLOGY

Parties involved in the completion of the DPIA

Briefly, the working team and the roles, tasks, responsibilities, etc. will be described.

In general, the team will be multidisciplinary and will respond to the context in which the DPIA is completed and the processing takes place, a context which may include regulatory, social or cultural questions, geopolitical, etc.

In the event that processing involves the use of emerging or innovative technologies, the team must incorporate members with a technological profile capable of describing the scope, from a functional perspective and from the perspective of the potential impact on privacy, of the technology used.

Guidelines, tools, methodologies, standards and rulings used in the evaluation

Details on the methodologies used and justification of their selection, including compulsory standards, if any, regarding the way the DPIA is carried out in this specific processing operation.

Those rulings, sentences, resolutions or legal reports that might be taken into account as possible criteria applicable to processing or any of the aspects of processing in any of their phases will also be included.

Scope and limits of the DPIA: Identify what remains outside the scope of the assessment

Reasons must be provided for limiting the scope of the DPIA including those aspects that would remain outside the scope and the possible risks associated with rights and freedoms of persons, including the way in which they might be tackled, and identification of the parties responsible in charge of them.

VI. ANALYSIS OF THE PROCESSING OPERATION

In this section, an analysis will be carried out to identify the risk elements for the rights and freedoms of natural persons that, directly or collateral, entails the processing.

For an effective study of the processing, it should be analysed, dividing it into steps or stages from the point of view of the data life cycle, by examining each of its stages separately.

In Appendix I of the AEPD's DPIA Guide there is a template for the possible segmentation of the processing operation into the so-called "life-cycle of the data associated with a processing operation."

It is recommended that at least the following phases are considered: data collection, classification and storage; use and processing or exploitation of the data; communications and transfers to third parties for processing; and the destruction of the data.

For each of these phases, identify the inherent risk elements for rights and freedoms of the data subjects in each stage, particularly:

- The proposals and direct and desired effects

- The possible collateral effects that might affect the fundamental rights and freedoms of citizens.

- Identify categories of data, interested parties, forms of collection and data enrichment.

- Extension in time, in space, on the specific group or on the information on a subject.

- Technologies and techniques employed and their uncertainty.

- Limitations to rights, access to services or other effects of a legal nature.

- Intervening parties and legal bases that legitimise such intervention in processing (contract, legal obligation, etc.)

- Etc.

The data are categorised in accordance with their common characteristics. A detailed study would analyse each data type on an individual basis or, if more practical, types of data can be grouped together.

VII. ANALYSIS OF THE OBLIGATION TO COMPLETE A DPIA: RISK ASSESSMENT

Inclusion of processing operation in the list of exempt processing operations

If the processing operation is included on the list of exempt processing operations as established in the framework of Article 35.5 of the GDPR, it is not compulsory to complete the DPIA and the report would end here. Otherwise the reasons why controller has taken the decision to complete an impact assessment should be provided subsequently (see section Reasons to Carry out a DPIA).

That list, approved by the European Data Protection Board, can be consulted here and is of a purely indicative nature.

Analysis of obligation to complete DPIA for the processing operation

In this section it will be determined whether or not there is an obligation to complete the DPIA. In order to do so, it must be considered whether the processing operation:

- Is included on the list of cases set out in Article 35.3 of the GDPR.
- Fulfils the conditions set out in the list of processing operations (Article 35.4 of the GDPR) for which it is compulsory to carry out a DPIA. That list, approved by the European Data Protection Board, can be consulted here and is of a purely indicative nature.
- Meets the high risk situations for cases listed in Article 28.2 of the LOPDGDD.

Assessment of level of risk

In this section, the level of risk is assessed, even if the processing operation is not included in the cases requiring compulsory completion of a DPIA.

It is necessary to complete an intrinsic risk analysis, in accordance with Article 35.7.c of the GDPR, taking into account the elements identified in the chapter "Analysis of the Processing Operation" to determine and identify the risks to people's rights and freedoms, both those inherent in the processing operation and those arising from the environment in which the processing operation takes place.

Each of the identified risk elements must be listed and subsequently managed in section IX "Measures for risk reduction".

As a result, we must measure the level of risk of the processing operation.

VIII. ANALYSIS OF THE NEED FOR THE PROCESSING OPERATION

The purpose of this section is to establish:

- Suitability: whether or not the processing operation can achieve the proposed objectives.

- Necessity: determine if the processing operation is necessary or whether there is another way of achieving the objective with the same or reasonable efficiency that is less invasive of privacy.

Benefits for data subjects

In this section, the direct benefits for society as a whole, stakeholder groups and for the specific data subjects in question must be identified. It will be necessary, therefore, to determine whether in this specific case, whether the following benefits apply:

- Direct and objective benefits for the subject under risk.
- Benefits for society overall
- Better service for all citizens and/or low risk subjects
- Greater accessibility to information.
- Greater environmental sustainability
- Greater transparency in the processing of data

- Substantial improvement in the health of citizens and/or low risk subjects
- Assistance and protection for persons in risk or disadvantaged situations.
- Protection from threats to State security, defence or public safety.
- To increase the efficiency of services to citizens and/or low risk subjects
- More accessible and integrated public services.
- To reduce discrimination (based on gender, age, nationality, disability, etc.)
- To empower data subjects.

Benefits for the entity or public administrations in general

This section includes the benefits of the implementation of the processing operation for the entity itself.

- Regulatory compliance
- Improvement of efficiency
- Reduction of costs
- Increase in the control of the activities of the Public Administrations
- Improvement in the transparency factor for the data controller
- Improvement of security of entities
- Improvement of image
- Corporate social responsibility goals
- Etc.

Alternatives to the processing operation and why they were not chosen

In cases of high-risk processing operations, this section must include an assessment of why other alternatives to the design and implementation of the processing operation that involve a lower risk were not chosen.

Where the reasons provided are the improvement, extension or modification of a processing operation, it is necessary to highlight the advantages of the new approach to processing and that the purpose sought cannot be achieved by other means, for example:

- Using other data

- Reducing the population of data subjects (in a qualitative or quantitative manner)

- Minimisation of the data collected, their use or conservation.

- Making use of other less invasive technologies

- Applying other procedures or forms of processing (amending those initially envisaged), etc.

For each alternative or previous form of proposed processing, it would be necessary to analyse:

- To what extent the advantages are changed for the entity responsible for the processing.
- To what extent the advantages for data subjects are changed
- To what extent risks to data subjects are changed.

- Finally, carry out a weighting of the alternative as opposed to the proposed processing operation and conclude with the reasons why it was ruled out.

IX. MEASURES TO REDUCE THE RISK

The purpose of this paragraph is to establish management, organization, processing, procedural and technical measures to manage each of the risk elements identified in Section VII "Analysis of the obligation to carry out DPIA: risk Assessment".

Optimising the processing operation

From a data protection perspective, the breakdown of the processing operation description into phases or sub-processes must be optimal in order to apply the measures to reduce risk at a more level of granularity.

Thus, any potentially unnecessary phases should also be identified, isolating those with highest levels of risk from the other phases, determining specific measures to manage the phases with the highest levels of risk and determining those that do not require access to personal data.

Privacy by design and default (PBDD) measures

The Privacy by Design and Default (PBDD) measures applicable will depend on the type of processing operation. Moreover, specific measures will be applied in the different phases of the processing operation and, therefore, the application of these measures is related to the previous section "Optimising the processing operation".

In order to resolve this paragraph, it is advisable to consult, in particular, A Guide to Privacy by Design published by the AEPD, and in general, guidelines and notes published on the AEPD website under Innovation and Technology.

A non-exhaustive list of measures for generic processings, derived from what is set in Article 25 of the GDPR, such as:

- MINIMISATION
- Early deletion of unnecessary data
- Minimisation of data collected and processed in each phase of processing.
- Minimisation of frequency of collection of data, for example, in consumption readings, geolocation, etc.
- Reduction of precision/granularity in data collection, for example, information on events, position, etc.
- Limitation of accessibility of databases through the network
- Early anonymisation
- Pseudonymisation of stored data.
- Pseudonymisation of data in some sub-processing operations
- MASKING
- Early anonymisation

- Pseudonymisation of stored data.
- Pseudonymisation of data in some sub-processing operations
- Introduction of measures disruptive to data at source
- Control of privacy of metadata in electronic communications
- Use of credentials based on attributes
- Encryption of stored information or information in transit
- SEPARATION
- Compartmentalisation of access to data in real time
- Compartmentalisation of access to data between processing operations.
- Partitioning of attributes of databases
- Blocking of data
- Physical separation of data sources.
- AGGREGATION
- Generalisation of personal data
- Aggregation of registers
- Reduction of precision/granularity in data collection, for example, information on events, position, etc.
- Application of differences in the dissemination of and access to the results of the processing operation
- INFORMATION
- Transparency of the extent of processing for the data subject.
- Transparency regarding the moment when data collection is carried out
- CONTROL
- User control of the collection of personal data
- User control of the processing of personal data
- End-to-end encryption of information
- COMPLIANCE
- Set privacy requirements in the products/services acquired or assigned for development.
- Incorporate the development of processing operations that involve personal data the privacy requirements in the first phases of the life cycle.
- Implement procedures to guarantee the authenticity or quality of data
- Implementation of physical measures to limit the collection of data such as physical privacy masks on cameras, covers on webcams, etc.
- Maximum privacy configuration by default
- Special attention on the circumstances of data subjects at in situations of special risk or vulnerability
- Limitation of automatic processing of data involving automated decisions

Accountability measures

Accountability measures are those aimed at implementing a system of governance of the personal data that allows for the demonstration of compliance with:

-Principles

-Rights

-Guarantees to manage the risk

In particular:

-Measures that allow for control of the data accessed: whose, by who, when, with what legitimate purpose and what processing operations they have been subject to.

- Measures to ensure that the management systems of rights are executed adequately

- Measures to conserve the traceability of data communicated to third parties

- Measures to notify subjects of data security incidents affecting their rights and freedoms

- Human intervention on the part of the data controller in processing operations involving automated individual decisions

- etc.

Security Measures

This section details the analysis of the requirements necessary to minimise risks to the fundamental rights and freedoms of natural persons in relation to security domains, confidentiality, the availability, integrity, authenticity and traceability of data and how to integrate those requirements with the rest of the data and how the integration of said requirements with the rest of the security (to continue the business, fraud control, etc.) of the organisation.

It may be convenient to annex the document of the Declaration of Suitability signed by the Security Manager.

X. RISK-BENEFIT ANALYSIS

The purpose of this chapter is to make a Judgement of Proportionality in the strictest sense: to determine if the processing operation is to consider or balanced, deriving more benefits or advantages of general interest than damages to other goods or values in conflict.

The essence of the risk management is to achieve a good balance between costs and benefits, greatly contributing to senior management decision making.

Within the framework of a DPIA, the cost is translated into risks to the fundamental rights and freedoms to which the data subjects in question are subjected.

It is necessary, therefore, to strike a balance between the risks of the processing operation for data subjects and the benefits that this processing operation provides to society as a whole.

The purpose of the risk assessment and the measures applied to reduce risk also taking into account the benefits arising from the processing operation. Justify how the advantages of the processing operation for data subjects compensate the risks involved.

(It is assumed to be a cyclical process in which measures are applied to reduce said risks).

XI. ACTION PLAN

This chapter should reflect on the implementation plan for the measures and guarantees to manage risk and the monitoring actions for the effectiveness of same

A template for completing a basic action plan can be found in Appendix IV of the AEPD'S Data Protection Impact Assessment Guide.

The same document also details the objectives, tasks, calendar, the necessary resources, the parties responsible and the interaction with other processing organisations.

In particular, they must reflect the privacy measures by design and by default to ensure that data protection is an integral part of the product/service and not merely an added layer.

XII. CONCLUSIONS AND RECOMMENDATIONS

This chapter establishes the final result of the risk analysis, the general guidelines for the implementation of the processing operation, determining whether the risk is sufficiently low and assessing whether a Prior Consultation with the AEPD is appropriate in accordance with Article 36 of the GDPR.

XIII. APPENDICES

Those contracts, declarations, descriptions, reports, regulatory references, standards, guides or general documents relevant to the drafting of the results of this report and which are referred to in the text may be included in part or in full as appendices.

Date: ……..

On behalf of data controller

Mr./Mss.: ……

ANNEX II – Informed consent form template

The following template will be used/adapted as necessary for its use in the Tools4LEAs project, when organising events and or other activities at which information from the participating individuals will be collected.

Your participation in this [study/event] is voluntary. You can choose not to participate or to leave the [study/event] at any point without any negative consequences.

By participating in this [study/event], you confirm that:

- you are 18 years or older and competent to provide consent.
- you have read the information about this [study/event] and this informed consent procedure.
- you have been fully informed about the aims and purposes of the Tools4LEAs project; more information can be found at tools4leas.eactda.eu or requested at info@eactda.eu.
- you have been given the opportunity to ask questions regarding the purpose of the [study/event].
- you agree that your data collected in the [study/event] can be used for scientific purposes and that you have no objection that your data is published in project-related publications in a way that does not reveal your identity;

Information may be shared between any of the other team members participating in this project in an anonymous form. All information you give will be treated as confidential.

This consent form is made pursuant to the relevant national, European and international data protection laws and regulations and personal data treatment obligations. Specifically, this consent document complies with the EU General Data Protection Regulation (2016/679) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

ANNEX III – Social Impact Assessment template

The Social Impact Assessment (SIA) template presented below[8] intends to allow the Tools4LEAs project to have a clear and consistent approach to assessing social impacts. Hence, it aims to:

- Build higher levels of community understanding of projects.
- Help the community to understand what is required to meet the project's goals and expectations.
- Give stakeholders and the community confidence that their concerns and perspectives are being considered early in the assessment.
- Reduce project risks and costs related to unplanned or reactive management of social impacts.
- Create better project-community relations and more socially sustainable outcomes.
- Streamline assessments by reducing requests for more information.

PROJECT ACTIVITIES	Which **project activity / activities** could produce social impacts?	
CATEGORIES OF SOCIAL IMPACTS	what **social impact categories** could be affected by the project activities	
POTENTIAL IMPACTS ON PEOPLE	What impacts are likely, and what **concerns/aspirations have people expressed** about the impact? Summarise **how each relevant stakeholder group might experience the impact**. *NB. Where there are multiple stakeholder groups affected differently by an impact, or more than one impact from the activity, please add an additional row.*	
	Is the impact expected to be **positive or negative**	
PREVIOUS INVESTIGATION OF IMPACT	Has this **impact previously been investigated** (on this or another project/s)?	
	If "yes - this project," briefly describe the previous investigation. If "yes - other project," identify the other project and investigation	
CUMULATIVE IMPACTS	Will this **impact combine with others** from this project (think about when and where), and/or with impacts from other projects (cumulative)?	

[8] Based on the template provided by the NSW Government (https://www.planning.nsw.gov.au/Policy-and-Legislation/Under-review-and-new-Policy-and-Legislation/Social-Impact-Assessment - date of retrieval 2021-09-20)

	If yes, identify which other impacts and/or projects		
ELEMENTS OF IMPACTS - Based on preliminary investigation	Will the project activity (without mitigation or enhancement) **cause a material social impact** in terms of its: You can also consider the various magnitudes of these characteristics	**extent** i.e., number of people potentially affected?	
		duration of expected impacts? (i.e., construction vs operational phase)	
		intensity of expected impacts i.e., scale or degree of change?	
		sensitivity or vulnerability of people potentially affected?	
		level of concern/interest of people potentially affected?	
ASSESSMENT LEVEL FOR EACH IMPACT	Level of assessment for each social impact		
SIA METHODS	What **methods and data sources** will be used **to investigate this impact**?	Secondary data	
		Primary Data - Consultation	
		Primary Data - Research	
	What **methods** will be used to **investigate this impact**?		
PROJECT REFINEMENT	Has the project been **refined in response to preliminary impact evaluation** or stakeholder feedback?		
MITIGATION / ENHANCEMENT MEASURES	What **mitigation / enhancement measures** are being considered?		

ANNEX IV – Ethics Assessment template

If deemed appropriate, during the course of the Tools4LEAs project ethics assessments might be conducted to ensure that the project complies with the ethical principles described in section "5 Ethics Assessments". To facilitate those assessments, the following guidelines / template is proposed.

1) Context

Provide information about the Tools4LEAs project and the specific work being assessed to set the scene. Such information should include: funding, motivation, expected scientific outcomes, study design, methods used, reasons for this particular project being important, etc.

2) Overall Ethical Issues

Describe the ethical issues raised by the objectives of the Tools4LEAs project, its respective results or findings and the potential consequences of your research outcomes. Provide details about how the identified overall ethical issues will be addressed.

3) Participants

Provide details about how you will be recruiting participants (inclusion/exclusion criteria, sites of recruitment, process...) and how informed consent (procedure for informing people, choices offered...) will be obtained. See "ANNEX II – Informed consent form template" for further details.

4) Risks and Benefits to Stakeholders

Go through the list of all directly involved or indirectly affected groups of people discussing what the potential risks to them are (e.g., social, physical, psychological, financial...) and how they might benefit (e.g., reward, self-esteem, new skills, fun).

5) Data Collection and Privacy

Explain in detail which data you will be collecting, how you collect it, how it will be stored and secured and what measures will be taken to protect the privacy of people involved.

6) Legal Boundaries and Guiding Documents

What relevant ethical and legal documents apply to the proposed research and/or what ethical guidance documents will be relied on? In which ways will these documents apply?

7) Ethics Monitoring

Explain which structures or procedures you have in place to monitor ethics and to be able to react to ethical issues that were not foreseen in this document.

8) Conflict Resolution

What are the potential conflicts that may arise in the research (e.g., between stakeholders and researchers) and how are they to be solved?

9) Other Ethical Concerns

Present, if applicable, other ethical concerns that need to be addressed (for example, unintended uses of an application, findings unrelated to the study goals etc.).