Intelligence Network & Secure Platform for Evidence Correlation and Transfer

D8.5 Ethical, Legal and Social Requirements for the INSPECTr Platform and Tools

Document Summary Information

Grant Agreement No	833276	**Acronym**	INSPECTr
Full Title	**I**ntelligence **N**etwork & **S**ecure **P**latform for **E**vidence **C**orrelation and **Tr**ansfer		
Start Date	01/09/2019	**Duration**	42 months
Project URL	https://www.inspectr-project.eu		
Deliverable	D8.5 Ethical, Legal and Social Requirements for the INSPECTr platform and tools		
Work Package	WP 8		
Contractual due date	28.02.21	**Actual submission date**	11.01.22
Nature	R	**Dissemination Level**	PU
Lead Beneficiary	TRI		
Responsible Author	Dr Joshua Hughes		
Contributions from	Dr David Barnard-Wills, Dr Leanne Cochrane		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 833276.

Revision history (including peer reviewing & quality control)

Version	Issue Date	% Complete	Changes	Contributor(s)
v0.1	29.01.21	0	Initial Deliverable Structure	Leanne Cochrane
v0.2	29.01.21		Internal review	David Barnard-Wills, David Wright
v0.3	17.02.21		Peer review	Panos Protopapas
v0.4	22.02.21		Peer review	Daniel Camara
v0.5	22.02.21		EAB review	Daragh O Brien
v1.0	25.02.21	100	Revision following peer review and EAB review	Joshua Hughes
V1.1	16.12.21		Revisions following interim review	Joshua Hughes
V1.2	07.01.21		EAB review	Daragh o Brien
V2.0	10.01.21	100	Revision following EAB review	Joshua Hughes

Disclaimer

Copyright message

Table of Contents

List of Tables

Glossary of terms and abbreviations used

Abbreviation / Term	Description
AI	Artificial intelligence
AI HLEG	High-Level Expert Group on Artificial Intelligence
CFR	Charter of Fundamental Rights of the European Union
DPIA	Data Protection Impact Assessment
EAB	Ethics Advisory Board
EC	European Commission
ECHR	European Convention of Human Rights (ECHR)
EDPS	European Data Protection Supervisor
EGE	European Group on Ethics in Science and New Technologies
ELSI	Ethical, legal and social issues

EU	European Union
GDPR	General Data Protection Regulation
Ibid.	*Ibīdem* (reference is the same as the preceding one)
IEEE	Institute of Electrical and Electronic Engineers
LEA	Law Enforcement Authority
LED	Law Enforcement Directive
TFEU	Treaty on the Functioning of the European Union
TRI	Trilateral Research Ltd.
WP	Work Package

1 Introduction

The aim of this deliverable is to set out the ethical, legal and societal issues associated with the INSPECTr Platform and Tools during its envisaged operational use. Ethics requirements for INSPECTr as a *research project* have been detailed in a series of WP9 deliverables.

Whilst the majority of INSPECTr technologies being researched and developed will not be ready for operational deployment by the end of the project, design decisions will be made at this stage which impact upon their eventual use. The project is at a stage where it can generate and make use of a set of ethical design requirements.

The deliverable has been informed by the Ethics Governance processes and tools detailed in deliverable D8.1 and reflects the ethics requirements that should accompany the INSPECTr functional requirements at month 18 of the project. The identification of ethical, legal and societal issues is an ongoing activity during the course of the 42-month research project, during which time further requirements could be added.

1.1 Update following interim review

Following the Interim review, reviewers wrote: '*This deliverable needs to be contextualised for the project. For example, the 3rd BP on page 21 on traffic light mechanisms is not mentioned in any of the technical report. Page 22 talks about AI systems. However, there is no clear elaboration where the AI system in the project is and the role of AI in tools and components developed in the project. Section 5 page 25-30 is generic and needs to be contextualised for the project. The social aspects are not addressed in a meaningful way as per DoA page 133 ("Cataloguing the ethical, legal and social issues associated with the INSPECTr platform and how they should be addressed and resulting requirements for the design and development of the platform and tools"). An updated and more detailed version, including the missing analysis and explanations, is requested*.'

In response to this comment, Section 4.2 has been expanded to explain how implementation of the Traffic Light Protocol has evolved from the initial discussion in v1.0 of this deliverable to be a cross-platform mechanism.

With respect to the references to 'AI systems', it is specified in Section 4.4 that this refers to tools that are intended to automate tasks that previously required cognitive skills of human beings (e.g., crime prediction, profiling, NLP, facial recognition, object detection, and child detection tools).

In terms of social aspects, Section 3.3 has been updated to contextualise key issues to the INSPECTr project, note how INSPECTr is approaching key social issues, and to describe how social issues are being considered with respect to some of the INSPECTr tools raising most social issues.

Further, a general update on progress in fulfilling the ELS requirements in Section 5 has been provided.

1.1 Mapping INSPECTr Outputs

The purpose of this section is to map INSPECTr Grant Agreement commitments, both within the formal Deliverable and Task description, against the project's respective outputs and work performed.

Table 1: Adherence to INSPECTr GA Deliverable & Tasks Descriptions

INSPECTr GA Component Title	INSPECTr GA Component Outline	Respective Document Chapter(s)	Justification
DELIVERABLE			

D8.2.0 Ethical, legal and social requirements for the INSPECTr platform and tools	*Cataloguing the ethical, legal and social issues associated with the INSPECTr platform and how they should be addressed, and resulting requirements for the design and development of the platform and tools.*	*Sections 3, 4 and 5*	*Section 3 identifies high level ethical, legal and social issues as laid out in international standards, laws and policies.* *Section 4 identifies the key ethical, legal and social issues identified as relevant to INSPECTr at m18.* *Section 5 summarises the ethical, legal and social requirements that should accompany the functional requirements including a measure of their achievement.*
D8.1.1 First Report on Ethical Governance	*A report documenting the ethical management processes and any ethical issues experienced during the project.*	*All.*	*This deliverable sets out TRI's ethics governance processes and tools. These processes and tools are the mechanisms through which the ethical, legal and social issues in this document and associated requirements have been identified.*
TASKS			
T8.2 Ethical, legal and social issues and requirements for the INSPECTr Platform and Tools.	*This task will undertake a sociological examination of the main ethical, legal and social issues (ELSI) that are relevant to INSPECTr's technologies in their operational environments. Further ethical and societal aspects of gender will be reviewed…The partners will consult stakeholders to gather their views on the ELSI that might arise from within INSPECTr. The results will be a set of privacy and ethical requirements to be combined with the functional requirements.*	*Sections 3, 4 and 5*	*Section 3 identifies high level ethical, legal and social issues as laid out in international standards, laws and policies.* *Section 4 identifies the key ethical, legal and social issues identified as relevant to INSPECTr at m18.* *Section 5 summarises the ethical, legal and social requirements that should accompany the functional requirements including a measure of their achievement.*

1.2 Deliverable Overview and Report Structure

Section 2 sets out the methodology used to inform the ethics requirements in the deliverable.

Section 3 sets out the higher-level ethics requirements that should be applied throughout INSPECTr.

Section 4 focuses on the core ethics requirements that have emerged throughout the ethics governance processes that are in addition to the design safeguards applied in the original Platform proposal.

Section 5 collates the list of ethics requirements to accompany the functional requirements.

2 Methodology

The deliverable has been informed by the full remit of Ethics Governance processes and tools detailed in deliverable D8.2. It has however, been particularly informed by the Data Protection Impact Assessments (DPIAs) carried out for activities in Tasks T1.3, ST3.4.2, ST4.4.1 and ST4.4.2 during month 12 of the INSPECTr project and by three 'spotlight' workshops held January-June 2021.

These 'spotlight' workshops were on ethical, legal and social issues identified as especially important for ethical design through Trilateral's ethics governance processes across months 1 to 12 of the project. An external expert with both technical capacity and knowledge of ethical, legal and social issues was invited to attend each workshop, together with the technical partners and the INSPECTr Ethics Advisory Board (EAB). The aim of each workshop was to engage across disciplines in an open, informal and in-depth dialogue on the ethical issues identified with a view to practically specifying further design requirements.

The first workshop took place on 19 January 2021 and focused on the **integration of publicly available data, typically online data,** into the INSPECTr Platform. The project was joined by data protection expert Dr Thilo Gottschalk and discussed the importance of data minimisation and data storage limitations in this regard. Design solutions, such as the use of search filters and default settings were identified as granular ethics requirements for the Platform.

The second workshop took place on 26 January 2021 and focused on **artificial intelligence systems** within INSPECTr. The project was joined by ethics expert Phil Booth and discussed the importance of bias mitigation and the understand-ability of the artificial intelligence output for LEA investigators. Design solutions, such as adjustments to datasets, weightings for certainty and the importance of error identification were discussed with a view to adoption in the Platform. These workshops inform the ethics requirements for the Platform, that accompany the functional requirements. Both workshops had around 20 participants from across the consortium.

Since the original submission of this deliverable, a third project workshop on **gender and AI** took place on 9th June 2021. The project was joined by computer scientist and ethicist Dr Allison Gardner and discussion gender issues that could be raised by the project and technologies being developed within it. Design solutions, such as conducting a bias audit of algorithms to mitigate biases from tools trained on problematic datasets (e.g., Wikipedia corpora), and avoiding further development of an emotion detection tool, were identified as steps that could be taken to fulfil the requirements developed in the original version of this document.

3 Ethical, Legal and Social Issues – Standards Framework

This section provides an overview of the existing ethical, legal (data protection) and social factors that are recognised at EU level and are relevant to the INSPECTr project.[1] They serve as a basis for analysing and formulating the ethical, legal and societal requirements that need to be respected through the INSPECTr Platform and Tools development process.

3.1 Ethical Guidelines

Ethics and fundamental rights are given the highest priority in EU-funded research.[2] Article 19 of the regulation on Horizon 2020 lays down the ethical principles applicable to all research funded by the programme. According to Article 19:

> *1. All the research and innovation activities carried out under Horizon 2020 shall comply with ethical principles and relevant national, Union and international legislation, including the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights and its Supplementary Protocols. Particular attention shall be paid to* ***the principle of proportionality, the right to privacy, the right to the protection of personal data, the right to the physical and mental integrity of a person, the right to non-discrimination and the need to ensure high levels of human health protection.***
> *2. Research and innovation activities carried out under Horizon 2020 shall have* ***an exclusive focus on civil applications****.*[3]

Ethics review and appraisal is an integral part of the research proposal evaluation process by the European Commission (EC). All projects submitted to the EC are evaluated from the point of view of the ethical and social impact. The ethical issues are listed in the Horizon 2020 Programme Guidance to ethics self-assessment.[4] It includes questions on the use of human embryos/foetuses, participation of humans, use of human cells/tissues, personal data, animals, involvement of non-EU countries, as well as questions on environment, health and safety, dual use and misuse.[5] A small number of these issues apply to INSPECTr.

INSPECTr aims to help Law Enforcement Agencies (LEAs) to enhance security through fighting organised crime and terrorism. The **2014 Opinion on the ethics of security and surveillance technologies issued by the European**

[1] This section is supported by Trilateral Research Ltd. research across H2020 FCT projects, notably COPKIT deliverable D2.4.
[2] European Parliament and the Council, Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 – the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC, 11.12.2013.
http://ec.europa.eu/research/participants/data/ref/h2020/legal_basis/fp/h2020-eu-establact_en.pdf
[3] Emphasis added. European Parliament and the Council, Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11
December 2013 establishing Horizon 2020 – the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC, 11.12.2013.
http://ec.europa.eu/research/participants/data/ref/h2020/legal_basis/fp/h2020-eu-establact_en.pdf
[4] European Commission, 'Horizon 2020 Programme Guidance How to complete your ethics self-assessment', Version 6.1– 04.02.2019, http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-selfassess_en.pdf
[5] Ibid.

Group on Ethics in Science and New Technologies (EGE) addresses the issues of security and surveillance technologies from an ethical perspective.[6] EGE is an independent, multi-disciplinary body which advises on all aspects of Commission policies where ethical, societal and fundamental rights issues intersect with the development of science and new technologies.[7] EGE emphasises the importance of dignity in the debate on security and surveillance. The core ethical principles on security and surveillance are the following: **privacy and freedom, autonomy and responsibility, well-being and/or human flourishing, and justice**.[8] Moreover, the EGE raises attention to procedural principles, which must be added in order to enable trust between individuals and companies and the state and/or states: transparency, efficacy and proportionality.[9] These principles help to establish security and principles that lead to restraints regarding security and surveillance instruments. These principles guide the regulation and practice of human rights protection in the area of security.[10]

In the context of INSPECTr, particular attention should be paid to guidance on research related to artificial intelligence (AI) and machine learning (ML). The European AI strategy places trust as a prerequisite to ensure a human-centric approach to AI.[11] As emphasised in the EC's Communication 'AI is not an end in itself, but a tool that has to serve people with the ultimate aim of increasing human well-being'.[12] The EC has appointed 52 experts to a High-Level Expert Group on Artificial Intelligence (AI HLEG), comprising representatives from academia, civil society, as well as industry to make recommendations on future related policy development and on ethical, legal and societal issues related to AI, including socio-economic challenges.[13] In April **2019, the AI HLEG presented the Ethics Guidelines for Trustworthy AI.**[14] Trustworthy AI has three components, which should be met throughout the system's entire life cycle: (1) it should be lawful, complying with all applicable laws and regulations (2) it should be ethical, ensuring adherence to ethical principles and values and (3) it should be robust, both from a technical and social perspective since, even with good intentions, AI systems can cause unintentional harm.[15] Based on fundamental rights and ethical principles, the document sets out seven key requirements that AI systems should meet in order to be trustworthy:

> **1. Human agency and oversight:** AI systems should support human autonomy and decision making, as prescribed by the principle of respect for human autonomy. This requires that AI systems should both act as enablers to a democratic, flourishing and equitable society by supporting the user's agency and foster fundamental rights and allow for human oversight. In situations where AI may negatively affect

[6] European Group on Ethics in Science and New Technologies (European Commission), 'Ethics of security and surveillance technologies', 20 May 2014, https://op.europa.eu/en/publication-detail/-/publication/6f1b3ce0-2810-4926-b185-54fc3225c969/language-en/format-PDF/source-77404258

[7] European Commission, European Group on Ethics in Science and New Technologies (EGE), https://ec.europa.eu/info/research-and-innovation/strategy/support-policy-making/scientific-support-eu-policies/europeangroup-ethics-science-and-new-technologies-ege_en

[8] European Group on Ethics in Science and New Technologies (European Commission), 'Ethics of security and surveillance technologies', 20 May 2014, https://op.europa.eu/en/publication-detail/-/publication/6f1b3ce0-2810-4926-b185-54fc3225c969/language-en/format-PDF/source-77404258

[9] Ibid.

[10] Ibid.

[11] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Building Trust in Human Centric Artificial Intelligence (COM(2019)168), 8 April 2019, https://ec.europa.eu/digital-single-market/en/news/communication-building-trust-humancentric-artificial-intelligence

[12] Ibid.

[13] European Commission, High-Level Expert Group on Artificial Intelligence, https://ec.europa.eu/digital-singlemarket/en/high-level-expert-group-artificial-intelligence

[14] High-Level Expert Group On Artificial Intelligence, 'Ethics Guidelines For Trustworthy AI', 8 April 2019, https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

[15] Ibid.

fundamental rights, a fundamental rights impact assessment should be undertaken. Users should be able to make informed autonomous decisions regarding AI systems. Human oversight may be achieved through governance mechanisms such as a human-in-the-loop (HITL), human-on-the-loop (HOTL) or human-in-command (HIC) approach. 'HITL refers to the capability for human intervention in every decision cycle of the system, which in many cases is neither possible nor desirable. HOTL refers to the capability for human intervention during the design cycle of the system and monitoring the system's operation. HIC refers to the capability to oversee the overall activity of the AI system (including its broader economic, societal, legal and ethical impact) and the ability to decide when and how to use the system in any particular situation.'[16]

2. Technical robustness and safety: A crucial component of achieving trustworthy AI is technical robustness, which is closely linked to the principle of prevention of harm. AI systems, like all software systems, should be protected against vulnerabilities that can allow them to be exploited by adversaries, e.g., by hacking. AI systems should have safeguards that enable a fallback plan in case of problems. Moreover, AI requires a high level of accuracy, which pertains to an AI system's ability to make correct judgements, for example, to correctly classify information into the proper categories, or its ability to make correct predictions, recommendations, or decisions based on data or models. It is also critical that the results of AI systems are reproducible, as well as reliable.

3. Privacy and data governance: AI systems must guarantee privacy and data protection throughout a system's entire lifecycle. The quality of the data sets used is paramount to the performance of AI systems. When data is gathered, it may contain socially constructed biases, inaccuracies, errors and mistakes. Such issues need to be addressed prior to training any given data set. In addition, the integrity of the data must be ensured. In any organisation that handles individuals' data (whether someone is a user of the system or not), data protocols governing data access should be put in place.

4. Transparency: AI transparency encompasses traceability, explainability and communication. The data sets and the processes that yield the AI system's decision, including those of data gathering and data labelling as well as the algorithms used, should be documented to the best possible standard to allow for traceability and an increase in transparency. This also applies to the decisions made by the AI system. This enables identification of the reasons why an AI-decision was erroneous which, in turn, could help prevent future mistakes. Traceability facilitates auditability as well as explainability. Explainability concerns the ability to explain both the technical processes of an AI system and the related human decisions (e.g., application areas of a system). Technical explainability requires that the decisions made by an AI system can be understood and traced by human beings. AI systems should not represent themselves as humans to users; humans have the right to be informed that they are interacting with an AI system. The AI system's capabilities and limitations should be communicated to AI practitioners or end-users.

5. Diversity, non-discrimination and fairness: Trustworthy AI must enable inclusion and diversity throughout the entire AI system's life cycle, ensuring equal access through inclusive design processes as well as equal treatment. This requirement is closely linked with the principle of fairness. Trustworthy AI requires avoidance of unfair bias, accessibility and universal design and stakeholder participation. Data sets used by AI systems (both for training and operation) may suffer from the inclusion of inadvertent historic bias, incompleteness and bad governance models. This could lead to unintended (in)direct prejudice and discrimination against certain groups or people, potentially exacerbating prejudice and marginalisation. The way in which AI systems are developed (e.g., algorithms' programming) may also suffer from unfair bias. This could be counteracted by putting in place oversight processes to analyse and address the system's purpose, constraints, requirements and decisions in a clear and transparent manner. Moreover, hiring from diverse backgrounds, cultures and disciplines can ensure diversity of opinions and should be encouraged. AI systems should not have a one-size-fits-all approach and should

[16] Ibid.

consider Universal Design principles addressing the widest possible range of users, following relevant accessibility standards. It is advisable to consult stakeholders who may directly or indirectly be affected by the system throughout its life cycle.

6. Societal and environmental well-being: Sustainability and ecological responsibility of AI systems should be encouraged, and research should be fostered into AI solutions addressing areas of global concern, such as the UN's Sustainable Development Goals. Ideally, AI systems should be used to benefit all human beings, including future generations. The effects of AI on people's physical and mental wellbeing, society and democracy must be carefully monitored and considered.

7. Accountability: Trustworthy AI necessitates mechanisms to ensure responsibility and accountability for AI systems and their outcomes, both before and after their development, deployment and use. It requires (a) auditability, which entails the enablement of the assessment of algorithms, data and design processes, (b) minimisation and reporting of negative impacts though impact assessments used (e.g., red teaming or forms of algorithmic impact assessment) both prior to and during the development, deployment and use of AI systems, (c) trade-offs should be addressed in a rational and methodological manner within the state of the art, (d) when unjust adverse impact occurs, accessible mechanisms should be foreseen that ensure adequate redress.[17]

In July 2020, the AI HLEG released **a self-assessment list** to help AI developers assess their tools against the Ethics Guidelines for Trustworthy AI.[18] This list should guide all AI developers through INSPECTr.

Finally, the Institute of Electrical and Electronic Engineers (IEEE), a global professional organisation working towards technology standards for human benefit, have a global Initiative on the ethics of autonomous and intelligent systems. In **2019, the IEEE released Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems** outlining a number of general principles to guide technology developers in the design and implementation of autonomous and intelligent systems (A/IS).[19] These principles are as follows:

1. Human Rights. A/IS shall be created and operated to respect, promote, and protect internationally recognized human rights.

2. Well-being. A/IS creators shall adopt increased human well-being as a primary success criterion for development.

3. Data Agency. A/IS creators shall empower individuals with the ability to access and securely share their data, to maintain people's capacity to have control over their identity.

4. Effectiveness. A/IS creators and operators shall provide evidence of the effectiveness and fitness for purpose of A/IS.

5. Transparency. The basis of a particular A/IS decision should always be discoverable.

6. Accountability. A/IS shall be created and operated to provide an unambiguous rationale for all decisions made.

7. Awareness of Misuse. A/IS creators shall guard against all potential misuses and risks of A/IS in operation.

[17] Ibid.

[18] AI HLEG, Assessment List For Trustworthy Artificial Intelligence (Altai) for self assessment, July 2020. https://ec.europa.eu/digital-single-market/en/news/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment

[19] The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems. Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems, First Edition. IEEE, 2019. https://standards.ieee.org/content/ieee-standards/en/industry-connections/ec/ autonomous-systems.html

8. Competence A/IS creators shall specify and operators shall adhere to the knowledge and skill required for safe and effective operation.

3.2 Legal (Data Protection) Guidelines

Human dignity expresses the intrinsic worth and fundamental equality of all human beings.[20] Human dignity significantly is the subject of the first Article of the Charter of Fundamental Rights of the European Union, which states that 'Human dignity is inviolable. It must be respected and protected'.[21]

Privacy plays a central role in the ethical and legal debate on security and is intricately connected to dignity.[22] The protection of natural persons in relation to the processing of personal data is a fundamental right described in Article 16(1) of the Treaty on the Functioning of the European Union (TFEU).[23] TFEU provides that everyone has the right to the protection of personal data concerning them. Moreover, protection of personal data is ensured in Article 8 of the Charter of Fundamental Rights of the European Union (the 'Charter'):

> *1. Everyone has the right to the protection of personal data concerning him or her.*
> *2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
> *3. Compliance with these rules shall be subject to control by an independent authority.*

The right to privacy is not an absolute right. Article 52(1) of the Charter accepts that limitations may be imposed on the exercise of rights such as those set out in Article 8 of the Charter. Nevertheless, limitations must be provided for by law, respect the essence of those rights and freedoms and, subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others.[24]

The EU legal framework ensures a high standard on data protection. The two major European legal acts applicable to INSPECTr's activities are the General Data Protection Regulation (GDPR) and the Law Enforcement Directive, which set forth numerous provisions that need to be respected.

The General Data Protection Regulation (GDPR)[25] regulates data protection and privacy for all individuals in the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR requires the implementation of measures to ensure data protection by design and by default. The GDPR aims to strengthen individuals' fundamental rights in the digital age and give

[20] European Group on Ethics in Science and New Technologies (European Commission), 'Ethics of security and surveillance technologies', 20 May 2014, https://publications.europa.eu/en/publication-detail/-/publication/6f1b3ce0-2810-4926-b185-54fc3225c969

[21] Charter Of Fundamental Rights Of The European Union, 2012/C 326/02

[22] European Group on Ethics in Science and New Technologies (European Commission), 'Ethics of security and surveillance technologies', 20 May 2014, https://publications.europa.eu/en/publication-detail/-/publication/6f1b3ce0-2810-4926-b185-54fc3225c969

[23] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, 2012/C 326/01

[24] Ibid.

[25] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

control over their personal data.[26] Moreover, the GDPR intends to facilitate business by clarifying the regulatory environment for companies and public bodies within the EU.[27]

The GDPR defines personal data as:

> *any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.*[28]

Under the GDPR, processing of personal data is determined as:

> *any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.*[29]

The GDPR outlines six data protection principles for processing personal data.[30] These principles relate to:

- **Lawfulness, fairness and transparency** – personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- **Purpose limitation** – personal data must be collected only for a specific, explicit and legitimate purpose. The purpose must be clearly stated. Organisations should only collect data for as long as necessary to complete that purpose. Processing that is done for archiving purposes in the public interest or for scientific, historical or statistical purposes is given more freedom.
- **Data minimisation** – personal data which is processed must be adequate, relevant and limited to what is necessary in relation to processing purpose. These data protection principles link with the concept of proportionality in a privacy context.
- **Accuracy** – organisations must take every reasonable step to update or remove data that is inaccurate or incomplete. Individuals have the right to request that inaccurate or incomplete data be erased or rectified within 30 days.
- **Storage limitation** – personal data must be deleted or anonymised when it is no longer needed. The timescales in most cases vary depending on circumstances and the reasons why this data is collected.
- **Integrity and confidentiality** – personal data must be kept safe and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In the context of intelligence-led preventive tools, the definition of profiling is of interest. The GDPR determines 'profiling' as:

---

[26] European Commission, 'Data protection in the EU', https://ec.europa.eu/info/law/law-topic/data-protection/data-protectioneu_en

[27] Ibid.

[28] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[29] Ibid, Article 4(2).

[30] Ibid, Article 5.

> *any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movement.*[31]

Moreover, Article 22 of the GDPR establishes rules for automated individual decision-making, including profiling:

> *1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.*
> *2. Paragraph 1 shall not apply if the decision:*
> *a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;*
> *b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or*
> *c) is based on the data subject's explicit consent.*
> *3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.*

Under the GDPR, a data protection impact assessment (DPIA) is mandatory for processing operations that are likely to 'result in a high risk to the rights and freedoms of natural persons',[32] especially when they involve new technology. These include in particular:

> *a) a 'systematic and extensive' analysis of personal data in the context of automated processing, including profiling, where this has a significant effect on the data subject;*
> *b) large-scale processing of 'special categories' of personal data, or of personal data relating to criminal convictions and offences; or*
> *c) a systematic monitoring of a publicly accessible area on a large scale.*[33]

The INSPECTr project responds to the European Agenda on Security, which prioritises terrorism, organised crime and cybercrime as interlinked areas with a strong cross-border dimension.[34] The exchange of data is essential in the fight against terrorism and cross-border crime. Nevertheless, effective law enforcement requires efficient and robust rules on personal data exchanges at national, European and international level.[35] The Law Enforcement Directive (LED)[36] is part of the new EU's data protection rules adopted in April 2016. The Directive is designed to be consistent with the GDPR.[37] The LED protects individuals when their personal data are

[31] Ibid, Article 4(4).
[32] Ibid., Article 35(1)
[33] Ibid., Article 35(3)
[34] European Commission, The European Agenda On Security, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions COM(2015) 185
[35] European Commission, 'Factsheet: How will the data protection reform help fight international crime?', January 2016
[36] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
[37] European Data Protection Supervisor, 'Police Directive'. https://edps.europa.eu/data-protection/our-work/subjects/policedirective_en

processed by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or for the execution of criminal penalties.[38] Under the LED, personal data must be processed lawfully, fairly, and only for a specific purpose, which is always linked to the fight against crime.[39] The LED provides that personal data processing across the EU complies with the principles of legality, proportionality and necessity, with appropriate safeguards for individuals.[40] Police and criminal justice authorities are bound by the principles of data protection by design and by default at the beginning of any process to do with personal data, for example, when developing new databases.[41] According to Article 5, Member States shall establish appropriate time limits and procedural measures for the erasure of personal data or for a periodic review of the need for the storage of personal data.[42] Furthermore, the LED ensures accountability of those responsible for processing personal data. The LED requires independent supervision by national data protection authorities and effective judicial remedies.[43] For instance, authorities must appoint data protection officers to take care of personal data protection within their organisation.[44] They must also ensure the national supervisory authority is notified of serious data breaches.[45]

The LED is consistent with the GDPR, therefore, it defines personal data and processing in the same manner as the GDPR. However, Article 6 of the LED obliges the controller to differentiate between different categories of data subject, such as:

> *a) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;*
> *b) persons convicted of a criminal offence;*
> *c) victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; and*
> *d) other parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts or associates of one of the persons referred to in points (a) and (b).*[46]

The LED protects special categories of personal data from processing:

> *Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Directive does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. Such personal*

[38] European Commission, 'Factsheet: How will the data protection reform help fight international crime?', January 2016
[39] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
[40] Ibid.
[41] European Commission, 'Factsheet: How will the data protection reform help fight international crime?', January 2016
[42] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
[43] Ibid.
[44] Ibid.
[45] Ibid.
[46] Ibid.

> *data should not be processed, unless processing is subject to appropriate safeguards for the rights and freedoms of the data subject laid down by law and is allowed in cases authorised by law; where not already authorised by such a law, the processing is necessary to protect the vital interests of the data subject or of another person; or the processing relates to data which are manifestly made public by the data subject. Appropriate safeguards for the rights and freedoms of the data subject could include the possibility to collect those data only in connection with other data on the natural person concerned, the possibility to secure the data collected adequately, stricter rules on the access of staff of the competent authority to the data and the prohibition of transmission of those data.*[47]

Moreover, the provisions regarding automated processing and profiling are crucial for the purposes of developing INSPECTr tools:

> *In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system.*
> *The data subject should have the right not to be subject to a decision evaluating personal aspects relating to him or her which is based solely on automated processing and which produces adverse legal effects concerning, or significantly affects, him or her. In any case, such processing should be subject to suitable safeguards, including the provision of specific information to the data subject and the right to obtain human intervention, in particular to express his or her point of view, to obtain an explanation of the decision reached after such assessment or to challenge the decision. Profiling that results in discrimination against natural persons on the basis of personal data which are by their nature particularly sensitive in relation to fundamental rights and freedoms should be prohibited under the conditions laid down in Articles 21 and 52 of the Charter.*[48]

3.2.1 Other relevant sources

The European Data Protection Board (EDPB) was established by the GDPR to ensure the consistent application of the GDPR and of the LED throughout the EU, and to promote cooperation between the EU's data protection authorities.[49] The EDPB regularly provides general guidance (including guidelines, recommendations and best practice) to clarify the law, advises the European Commission on any issue related to the protection of personal data and new proposed legislation in the European Union, and adopts consistency findings in cross-border data protection cases.[50]

Some of the EDPB's opinions and guidelines are relevant to the development of INSPECTr's tools, for instance, guidelines on automated individual decision-making and profiling[51] and guidelines on data protection impact assessment (DPIA) and determining whether processing is 'likely to result in a high risk.'[52]

The EDPB has replaced the Article 29 Working Party (WP29), which was the independent European working party that dealt with issues relating to the protection of privacy and personal data. On 29 November 2017, WP29

[47] Ibid.
[48] Ibid.
[49] European Data Protection Board, https://edpb.europa.eu/about-edpb/about-edpb_en
[50] Ibid.
[51] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053
[52] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

adopted 'Opinion on some key issues of the LED (EU 2016/680)', which provides guidance by recommendations and remarks on the issues relevant for the INSPECTr project: time limits for storage and review; processing special categories of personal data; automated individual decision making and profiling; rights of the data subject; logging; powers of data protection authorities.[53]

Another document that may serve as a reference point for INSPECTr is about ethics and data protection issues raised by the panel of experts at the request of the European Commission (DG Research and Innovation).[54] The document aims at raising awareness in the scientific community, and in particular with beneficiaries of EU research and innovation projects.[55] The authors emphasise that the fact that research is legally permissible does not necessarily mean that it will be deemed ethical.[56]

3.3 Social Values

The European Union (EU) is a community of values. The EU is **founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities and people with disabilities**.[57] These values are embedded in the European Convention of Human Rights (ECHR) and the Charter of Fundamental Rights of the European Union structured around the principles of dignity, freedom, equality, solidarity, citizens' rights and justice.[58] The charter brings together the personal, civic, political, economic and social rights enjoyed by people within the EU.[59] To reflect modern society developments, the charter includes 'third generation' fundamental rights, such as data protection.[60]

When exploring social values at the EU level, it is worth to look at the Eurobarometer data. In the context of security, according to a special Eurobarometer on Europeans' attitudes towards security (April 2015), establishes how secure European citizens feel, what they regard as the main security threats to the EU, and which organisations or institutions are best placed to address these challenges, and whether these groups are doing a good job in tackling security threats.[61] A substantial majority of Europeans feel secure, whether in their

[53] Article 29 Data Protection Working Party, 'Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)', 29 November 2017, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48804
[54] Ethics and data protection, 14 November 2018, http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf
[55] Ibid.
[56] Ibid.
[57] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Building Trust in Human Centric Artificial Intelligence (COM(2019)168), 8 April 2019, https://ec.europa.eu/digital-single-market/en/news/communication-building-trust-humancentric-artificial-intelligence
[58] European Commission, The Charter of Fundamental Rights, https://ec.europa.eu/info/aid-development-cooperationfundamental-rights/your-rights-eu/eu-charter-fundamental-rights/why-do-we-need-charter_en
[59] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Building Trust in Human Centric Artificial Intelligence (COM(2019)168), 8 April 2019. https://ec.europa.eu/digital-single-market/en/news/communication-building-trust-humancentric-artificial-intelligence
[60] Charter of Fundamental Rights of the European Union, 2012/C 326/02
[61] Special Eurobarometer 432, "Europeans' attitudes towards security", conducted by TNS Opinion & Social at the request of the European Commission, Directorate-General for Migration and Home Affairs, April 2015

immediate neighbourhood or in the EU as a whole.[62] Respect for fundamental rights and freedoms is thought to have the most positive impact on one's personal sense of security.[63] Yet, a majority of respondents think that citizens' rights and freedoms have been restricted for reasons related to fighting terrorism and crime.[64] In terms of INSPECTr, this indicates that the project is correct to include specific considerations of ethics, privacy, and fundamental rights as a key part of the project and to ensure that these standards are upheld and citizens are protected.

Terrorism is perceived as the EU's most important security challenge. However, the level of concern varies considerably from country to country, e.g., 62% of people in Malta, but only 22% in Latvia, think terrorism is an important challenge.[65] Just under a quarter of people mention organised crime (23%).[66] Over two thirds of people think that the threat of terrorism is likely to increase over the next three years, with over half also saying that cybercrime and organised crime will increase.[67] Over half of the respondents think the police are doing enough to fight terrorism and drug trafficking, but less than half say enough is being done to fight other crimes.[68] In terms of specific crimes, the following percentage of respondents say they agree that the police and other law enforcement agencies are doing enough: 61% - fight terrorism; 53% - to fight drug trafficking; 46% - to fight cybercrime; 44% - to fight arms trafficking.[69] Whilst there are different opinions on what is most important, it is clear that the focus of INSPECTr on researching tools to assist in terrorism and organised crime investigations is appropriate in order to make a contribution to facilitating LEAs better dealing with these issues.

A great majority of respondents see the police and the judicial system as being chiefly responsible for ensuring the security of citizens.[70] However, 79% of respondents think that citizens themselves should play an important role in ensuring security.[71] This underlines the importance of the INSPECTr approach surveying LEA partners for their thoughts on issues related to the project and the technologies being researched, and also taking the concerns of citizens very seriously. Societal concerns are brought into the project through work such as the present analysis and, in particular, ST8.2.2 Horizon Scanning that involves researching emerging issues including those that could have impacts on the societal level. These are then brought to the consortium through ST8.2.3 Sensitisation of the Consortium, where particular issues are raised with the consortium and their impact on the INSPECTr project and/or tools are discussed. Where specific issues have warranted in-depth discussions, workshops have taken place to determine how the consortium can best take account of the issues and deal with them; these have covered topics such as online data, ethical AI and discrimination, and gender and AI.

These workshops are key areas where relevant societal issues have been taken into account. Discrimination and gender are obviously key areas to consider as the issues raised for these topics affect large proportions of our societies and roughly half of them in the case of gender. The workshops led to in-depth discussion of these topics which led to progress being made on dealing with these issues in INSPECTr. For example, agreements were made by partners that: tools such as web crawlers were only appropriate to be used by LEAs after the project, and should not be used during research work; specific steps should be taken to deal with bias, transparency, and explainability; that gender issues should be thoroughly considered to prevent unintentional harms (for more details, see Section 4.2.1 of D8.7 Privacy and Ethics-by-Design in the INSPECTr Platform).

[62] Ibid.
[63] Ibid.
[64] Ibid.
[65] Ibid.
[66] Ibid.
[67] Ibid.
[68] Ibid.
[69] Ibid.
[70] Ibid.
[71] Ibid.

People are generally positive about the impact of new technologies, but a quarter think they will have a negative impact on the security of citizens.[72] Just over half of the respondents think that the development of new technologies positively impacts the rights and freedoms as well as the security of citizens in the EU.[73] It is good for the INSPECTr project that citizens think new technologies have positive impacts on their security, rights, and freedoms. However, it is also important to deal with the considerable number of people holding an opposite view. Their valid concerns indicate that the INSPECTr approach to include Privacy and Ethics-by-design was correct. As explained in detail in D8.7 Privacy and Ethics by Design in the INSPECTr platform, the research into new technologies in INSPECTr includes consideration of privacy and ethical concerns, including those related to wider society as one of the ethical requirements considered specifically deals with societal wellbeing. By keeping such concerns in mind whilst researching the INSPECTr platform and tools, it is hoped that, where they are aware of the ethical approach to technology development, citizens will be able to understand that the risks of unlawful or unethical infringements upon their rights should be much lower where the INSPECTr tools are used, compared to tools developed without such concerns being considered.

The tools developed in INSPECTr are highly relevant to cybercrime. According to a Eurobarometer survey on Europeans' attitudes towards cyber security (September 2017), 87% of respondents consider cybercrime an important challenge to the internal security of the EU.[74] Nevertheless, less than half of the respondents (49%) think enough is being done by law enforcement authorities to tackle cybercrime.[75] When compared to different threats to national security being perceived as important, these results place cybercrime in the middle range, with terrorism being perceived as the biggest threat.[76] Misuse of personal data and the security of online payments are the most significant concerns of Internet users.[77] Therefore, it is good that INSPECTr is researching tools that will be able to help investigators enhance their investigative abilities to deal with cybercrime. By increasing the ability of investigators to deal with this sort of criminality, it should help contribute to reducing the pervasiveness of this sort of crime, and subsequently demonstrating to citizens that their safety from cybercrime has been increased.

In terms of processing of personal data, according to a Special Eurobarometer on Data protection (June 2015), most respondents accept that data collection is a part of modern life, so long as it remains within appropriate boundaries.[78] In this respect, seven in ten respondents think that their explicit approval should be required before any kind of personal information is collected and processed in all cases.[79] Moreover, the trust of Europeans in public and financial institutions to protect their personal data is significantly higher than for private corporations. Thus, one in two Europeans say they trust the European institutions to protect their personal information.[80] This is beneficial for INSPECTr. Firstly, where INSPECTr partners have engaged in data collection, this is from consenting volunteers – thereby meeting the desire of European citizens to give explicit approval for their data to be used. Second, the INSPECTr tools are being developed with the aim of exploiting them to European LEAs, which, as shown with these survey results, are trusted by European citizens to protect their

[72] Ibid.
[73] Ibid.
[74] Special Eurobarometer 464a, "Europeans' attitudes towards cyber security", conducted by TNS opinion & political at the request of the European Commission, Directorate-General for Migration and Home Affairs, September 2017
[75] Ibid.
[76] Ibid.
[77] Ibid.
[78] Special Eurobarometer 431, "Data protection", conducted by TNS Opinion & Social at the request of Directorate-General for Justice and Consumers (DG JUST), June 2015
[79] Ibid.
[80] Ibid.

personal data. As such, the use of INSPECTr by European LEAs should be trusted by most citizens from the perspective of data protection and privacy.

In September 2018, Europeans citizens were asked about the topics they see as priority for the European elections campaign.[81] According to the ranking of the themes which should be discussed as a matter of priority during the election campaign for the next European Parliament elections, the following issues related to INSPECTr have attracted the respondents: fight against crime (49%, first place in the ranking), which INSPECTr contributes to by researching tools for LEAs to use; promoting human rights and democracy (32%, sixth place in the ranking), which INSPECTr contributes to by ensuring the potential impacts of the INSPECTr tools being used are considered in depth within the project; security and defence policy (29%, eighth place in the ranking), as a project with purely civilian aims, INSPECTr does not contribute to defence policy but does deal with area of concern for security and intends to communicate policy recommendations in D1.5, D6.9, D6.10, and D6.11; protection of personal data (20%, 12th place in the ranking), INSPECTr monitors compliance with this area of legislation through the data management plan and ensures measures are taken to embed protection of personal data in the INSPECTr technologies through T8.3.[82]

Regarding more specific societal aspects of the INSPECTr project and platform, a major aim of the project is that the Living Lab experiments demonstrate that use of the INSPECTr platform and tools could have sped up investigations compared with other similar tools. This would contribute to more rapid justice through enabling the LEA portion of the criminal justice system to work faster in organised crime investigations. Reducing delays to justice is an important social issue as holding a trial within a 'reasonable time' is part of the right to a fair trial,[83] and, therefore, adequate justice. Where justice to victims is delayed, this is often seen as 'justice denied'. Indeed, the importance of timely justice for victims of wrongdoing is highlighted as far back as the Magna Carta in 1215.[84] The reason for its importance is that the longer it takes for justice to be delivered, the more likely it is that the benefit of that justice will be lost. A claimant or victim might die, suffer being wronged for longer than necessary, or struggle to move on with their life until they are heard in court. On the other side, an offender might remove assets, flee, or commit more crimes before justice is served. Further, the longer needed for a trial to take place, the more likely that evidence will degrade, and memories will become faulty and impair the ability of witnesses to accurately testify. Additionally, delays to justice undermine faith in the rule of law where justice is not seen to be done in a reasonable time frame.[85] INSPECTr can contribute to providing timely justice by speeding up the investigative process, thereby contributing to reducing delays in justice being served, and as a consequence of this, preventing undermining of the rule of law.

In order to deal with tools being developed in INSPECTr from the societal perspective, some key tools where societal issues need to be thought about will now be considered. Final details about these tools will be reported in D8.6 Ethical, Legal and Social requirements for the INSPECTr platform and tools – Final Report. Here a brief overview of web scraping, facial recognition, and crime forecasting tools will be provided.

Web scraping as a tool for criminal investigations is important in the modern world as significant amounts of criminality takes place online and evidence needs to be taken from online sources for investigations and court proceedings. This can create a social issue whereby personal data from large numbers of innocent people might be collected inadvertently, reducing the private space for societies members to operate within. This is clearly an area where the benefit of researching an investigative tool and the benefits of personal privacy for society need

[81] Public Opinion Monitoring, 'The European Parliament and the expectations of the European citizens', September 2018, http://www.europarl.europa.eu/at-your-service/files/be-heard/eurobarometer/2018/public-opinion-monitoring-at-a-glanceseptember-2018/en-plenary-insights-september-2018.pdf

[82] Ibid.

[83] Art.6, European Convention for the Protection of Human Rights and Fundamental Freedoms (adopted 4 November 1950, entered into force 3 September 1953) 213 UNTS 221

[84] '*To none will we sell, to none will we deny or delay right or justice*.', Clause 40, Magna Carta (1215 version).

[85] See Lord Dyson, MR, *Delay too often Defeats Justice*, Speech to the Law Society, 22 April 2015, paras.15-17.

to be considered and balanced. As noted above, partners decided in INSPECTr that web scrapping should not take place during the project, and the tool could only be used after the project. The benefit of engaging in web scraping during the research phase of INSPECTr is minimal and would present a significant privacy issue, thus balancing of social benefits here has an obvious result in favour of privacy.

With respect to facial recognition, this is a very controversial technology. There are key issues around privacy as people cannot easily hide their faces without drawing attention to themselves, and might not even know they are being monitored.[86] In some parts of the world, this is used for seemingly dystopian levels of monitoring of citizens.[87] However, there are benefits to LEA use of facial recognition for highlighting persons of interest who might otherwise be missed in an investigation.[88] There are also significant concerns regarding bias and potential discriminatory impacts from this technology too.[89] Such is the level of concern, many people and organisations have called for this technology to be banned, including the European Parliament.[90] As such, in order to overcome the concerns about discrimination and privacy and the benefits of contributing to public security need to be properly balanced. In INSPECTr, facial recognition is confined to being used with existing academic datasets in the project, should be subject to bias testing, and is being used to prioritise images for end-users, rather than to make decisions on their behalf. As such, this should lessen the privacy and discrimination impacts whilst facilitating the public security benefits if the tool is used in the future.

Crime forecasting is another tool that can raise social issues. Such technologies generally work by tracking historical data relevant to crime and estimating where crimes are likely to happen in future. However, there are several examples of this type of technology using data that might be relevant to crime that are also relevant to ethnicity, with this leading to racialised policing operations.[91] In order to deal with this social issue, it is important that the data being processed is the correct data – i.e., that which actually aligns with criminality, rather than data which is a proxy for something else.[92] As such, in INSPECTr, the crime forecasting tool is focussed on geographic areas where crimes are reported (see Section 2.3.5. of D4.8). This, to an extent, mitigates the social discrimination issues as location of criminality is not directly linked to ethnicity, or another personal characteristic. However, location can reveal other information. For example, histories of racialised policing policies that led to discriminatory over-policing of areas heavily populated by members of ethnic minorities can highlight those areas as having a high crime rate, when, actually, there is a high-detection rate for crimes and this skews the data and subsequent analysis. In order to deal with this, the crime forecasting tool in INSPECTr can be recalibrated regularly (even daily) with recent data so that the forecasts are as accurate as possible. Whilst this is not to say that this approach mitigates all issues, it is preferable to approaches including significant amounts of historical data, and the approach to dealing with bias and discrimination is an ongoing discussion. As not all issues can be dealt through recalibration, this is an ongoing operational risk that end-users should be made aware of so that they can actively evaluate results as they are generated to ensure a realistic understanding

[86] Silkie Carlo, Jennifer Krueckeberg, and Griff Ferris, Face Off, Big Brother watch, 2018. Available at: https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf

[87] Zhou Jiaquin, Drones, facial recognition and a social credit system: 10 ways China watches its citizens, South China Morning Post, 2018, Available at: https://www.scmp.com/news/china/society/article/2157883/drones-facial-recognition-and-social-credit-system-10-ways-china

[88] Irakli Beridze, Marjolein Smit-Arnold Bik, Kay Firth-Butterfield, and Cyril Gout, A Policy Framework for Responsible Limits on Facial Recognition, World Economic Forum, 2021.

[89] Alex Najibi, Racial Discrimination in Face Recognition Technology, Harvard University Science Policy Blog, 2020. Available at: https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/

[90] Melissa Heikkilä, European Parliament calls for a ban on facial recognition, Politico, 2021. Available at: https://www.politico.eu/article/european-parliament-ban-facial-recognition-brussels/

[91] Will Douglas Heaven, Predictive policing algorithms are racist. They need to be dismantled., MIT Technology Review, 2020. Available at: https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/

[92] David G. Robinson, The Challenges of Prediction: Lessons from Criminal Justice, I/S Journal, Vol.14, Issue 2, p.151, pp.175-176.

of them, even with daily recalibration. The ethical use of this technology hinges upon the frequency of calibration, and the quality of input data. If data is not accurate, not collectedly properly, or is not present, then the data underpinning the forecasting will be as representative as it could be, and the results of the forecasting are likely to be skewed.

4 Ethical, Legal and Societal Issues associated with the INSPECTr Platform and Tools

The principle objective of INSPECTr is to develop a shared intelligence platform and a novel process for gathering, analysing, prioritising and presenting key data to help in the prediction, detection and management of crime in support of multiple agencies at local, national and international level. The Platform aims to integrate a number of Tools to assist LEAs in analysing digital evidence. Detailed information on the design and architecture of the Platform can be found in other project deliverables, such as deliverable D1.2.0 setting out the functional requirements for the Platform. This section identifies the main ethical, legal and social issues for the design of the Platform and Tools. These are the issues that respond to the operational use of the INSPECTr Platform and Tools and extend beyond the numerous ethical requirements incorporated into the early design of INSPECTr communicated in the project proposal and ethics checks processes, e.g. the already-planned secure audit process facilitated through blockchain technology, restricted personal data processing and legal controls on the exchange of data, etc. The issues identified below have been identified through the various Ethics Governance activities and processes outlined in project deliverable D8.2.

4.1 Lawfulness

LEA use of the INSPECTr Platform and Tools must be in accordance with the law. The INSPECTr Platform and Tools will include a legislation library, the 'rules-based engine', covering the cross-border querying and exchange of LEA data. As with any technology, there remains the risk that LEAs could use the Platform and Tools for purposes beyond their permitted legal scope. This risk is overseen by the LEA itself and their existing processes of accountability, transparency and governance once the Platform and Tools are adopted. However, to mitigate this risk in the design of the Platform and Tools, technical partners should consider whether pop-ups and/or notifications are suitable before the use of the Platform as a whole, or indeed before the use of individual Tools, in which the LEA investigator must first agree to knowing a lawful basis for use before they can progress (akin to agreeing to a end-user licensing agreement with commercial software). This would be in addition to the fact that the INSPECTr Platform and Tools will log every LEA investigator action through blockchain technology providing a traceable account of all activity. The need for immutable recording of the processing of the digital evidence that can be queried is a design requirement to attest of the chain of custody integrity.

Associated requirement(s):

- Platform and Tools: Consider an initial pop-out whereby LEA agrees to lawful basis for use.
- Rules based engine should be accompanied by clear guidance on its limitations, concerning the varied nature of legal systems, the evolving nature of law, including case law.

4.2 Data Minimisation

The INSPECTr Platform, has the potential to gather and store significant amounts of personal data, including publicly available data through the use of the web scraper tool. While the Platform and Tools should only be used lawfully by LEAs, the Platform and Tools should be designed and developed to facilitate the principle of data minimisation by default, limiting the opportunity for LEAs to inadvertently exceed the data minimisation principle. In the context of the LED, this means that personal data processing should be 'adequate, relevant and not excessive in relation to the purposes for which they are processed'. This risk is potentially higher for the tools which integrate publicly available data, such as from online sources, than from the seized evidence data which LEAs will integrate into the platform. This risk can also increase when datasets are merged revealing

additional personal data. There is also a risk that the use of the Platform and Tools could result in data 'leakage' about an LEA investigation and the data subjects within, when INSPECTr Tools which integrate with the web are used. The INSPECTr Platform and Tools operate a federated data storage model, whereby LEA case file data is stored on the local LEA node.

Associated requirement(s):

- All INSPECTr analysers are disabled by default and are individually enabled by LEA senior personnel.
- Each INSPECTr analyser to be accompanied by detailed documentation regarding its functionality (including limitations) allowing senior LEA personnel to decide on the appropriateness of each release.
- All INSPECTr web-based analysers to be accompanied by a traffic light protocol to identify the security level of the data accessed, e.g., TLP:AMBER.
- Web Scraper Tool to encrypt collected data.
    - Developers and LEAs to consider which investigators decrypt data, and how, with a view to ensuring data minimisation.
- Web Scraper Tool to include filter functionality to provide for limited data gathering where appropriate.
    - Web scraper design team to consult LEAs on common judicial preferences on filtering to reflect the legal concept of proportionality (e.g. what are they typically allowed or not allowed to collect) and to reflect this as far as is possible in the technical design.
- Web Scraper Tool design team to consider how the project can avoid the unintentional gathering of personal data using filters, natural language processing or other methods where the data is located at unusual positions/points on a webpage.
- Computer Vision Tool functionality to be limited to data stored on the INSPECTr Platform.
- Suspect and Criminal Profiling Tool to be limited to data stored on the INSPECTr Platform.

With respect to the Traffic Light Protocol (TLP) suggested for the web scraper tool, since the first version of this deliverable was submitted, partners have agreed that the TLP will be implemented across the platform for end-users to determine. The TLP can be set for each observable (e.g., piece of evidence) by an end-user whenever an observable is added or analysed in INSPECTr. The TLP levels[93] display what level of sharing is appropriate for each observable. Further, an appropriate TLP level can be set for each tool when they are enabled, so that the tools that offer the most risks of intruding on privacy are limited. For example, if a disk image is highly sensitive, and should only be accessed by one person, it could be marked 'red'; then, only tools that can work with at TLP level red would function with this observable.

An additional, linked, function implemented in INSPECTr is 'Maximum Permissible Actions Protocol' (MAX PAP). This protocol uses the same rating system as the TLP,[94] but relates to how information received can be processed, taking operational security concerns into account. For example, a cybercrime unit examining a piece of malware

[93] TLP: RED - distributed to specific persons only.
TLP: AMBER - distributed to a limited group on a 'need-to-know' basis.
TLP: GREEN - distributed to a particular community only.
TLP: WHITE - distribution unlimited, subject to copyright regulations.

[94] PAP: RED - Non-detectable actions only. Recipients may not use PAP:RED information on the network. Only passive actions on logs, that are not detectable from the outside.
PAP: AMBER - Passive cross check. Recipients may use PAP:AMBER information for conducting online checks, like using services provided by third parties (e.g. VirusTotal), or set up a monitoring honeypot.
PAP: GREEN - Active actions allowed. Recipients may use PAP:GREEN information to ping the target, block incoming/outgoing traffic from/to the target or specifically configure honeypots to interact with the target.
PAP: WHITE - No restrictions in using this information.
See Raphaël Vinot, et al. MISP Taxonomies, GitHub, 2019. Available at: https://github.com/MISP/misp-taxonomies/blob/main/PAP/machinetag.json

that is PAP: RED would not conduct an online check (e.g., using VirusTotal) on the piece of malware in case attackers were monitoring online sources to determine if their malware is being investigated. These protocols can be tightly integrated with the INSPECTr case management system. More technical details about implementation the TLP and MAX: PAP will be included in technical deliverables, most likely those from WP3 discussing the Publish/Subscribe Engine.

4.3 Storage Limitation

While storage of personal data can be important for LEA investigations and evidence retention, especially concerning data on the dark web which is often temporary, extensive storage beyond which is necessary should be avoided. The LEAs adopting the INSPECTr Platform and Tools will be responsible for the deletion of collected personal data in a timely manner. In the design of the INSPECTr Platforms and Tools, technology partners should ensure that the deletion of data is accessible for LEAs.

Associated requirement(s):

- LEAs should be able to delete their data across the INSPECTr Platform and Tools with relative ease. This means that developers should ensure that data residue is avoided on the Platform and in Tools.
- The design team in consultation with LEAs should consider the automated deletion of data, with prompts alerting LEAs to proactively extend storage.
    - This is advised especially for INSPECTr network data that has been obscured, such as 'queries' between Member State LEAs.

4.4 Diversity, non-Discrimination and Fairness

Removing bias fully from INSPECTr's artificial intelligence (AI) systems is not considered possible. By 'AI systems', we are referring to the gadgets and analysers that are intended to be incorporated into the INSPECTr platform in order to automate some of the functions previously carried out by human LEA officers and analysts (e.g., crime prediction, profiling, NLP, facial recognition, object detection, and child detection tools).[95]

Whilst it might not be possible to eliminate bias, the project should make *every effort* to mitigate bias in the datasets and models relied on. INSPECTr AI systems rely on various types of data. The Crime Prediction Tool is built on existing (anonymised) LEA data which reflects the information held by the LEA in that member state. It is known however, that some types of crime are underreported, such as domestic abuse, whilst different segments of the population may have been subject to "under-" or "over-policing" in the past, with both issues distorting the LEA data. Similarly, the Computer Vision Tool relies on pre-existing facial image data sets which are known to underrepresent ethnic minorities, having subsequent impacts upon accuracy and reliability. This is sometimes further complicated where the differences between people whose data are classified by AI systems act as proxies for personal characteristics, and present bias that is not initially recognised. Efforts to mitigate bias within the INSPECTr AI systems must take account of known biases in datasets and make efforts to account for other potential bias. It is also important to note that making end-users aware of biases in AI models can only be effective in the operational context where end-users take steps to properly understand the model and interpret the results.

Associated requirement(s):

[95] Noting that one of the most common definitions of 'AI' is an approach to computing to try to make machines replicate human activities. See Margaret A. Boden, *AI: It's nature and future*, OUP, Oxford 2016. p.1.

- In the absence of unbiased models, where using pre-trained models, partners should prefer the use of models where bias is already known and assessed over models where no measure or assessment of bias is available.
- All AI systems must seek to adjust existing models for bias to the full extent feasible, e.g., available adjustment data.
- All AI systems must display possible bias or reporting issues, according to relative weights in the model, alongside the results of analysis.
    - Design teams to consider Bayesian or other related approaches for dealing with bias.
- Selection of technical solutions, or decisions about technical features, must take into account how bias may emerge during operational use and the real-world impacts that might arise from this.

The professional fields most relevant to the INSPECTr Platform and Tools, namely information technology, law enforcement and digital forensics, experience a known gender imbalance in favour of men. This imbalance also translates across the INSPECTr partners. For this reason, it is crucial that INSPECTr partners endeavour to the fullest extent to ensure that females and other gender identifications with the appropriate skillsets are included within the INSPECTr design and testing process. A third WP8 workshop was be held in June 2021 to discuss further the issue of gender and the related ethics requirements and how to progress them. However, additional imbalances across other personal characteristics such as ethnicity, socio-economic background, disability, physical appearance, and other personal characteristics could also have impacts.

Associated requirement(s):

- Representation of minority and marginalised groups is an evaluation criterion for participation in testing and capacity building workshops. This includes, but is not limited to: sex; gender; ethnicity; socio-economic background; disability, and; physical appearance.

4.5 Transparency and Explainability

Transparency and explainability are especially important features of AI systems. In light of the difficulties in removing biases fully from such systems, it is crucial that LEA decision-makers understand how the AI system derived its outputs and any weaknesses behind them. This information can be communicated in a model agnostic manner but it must be accessible to the LEA and provide sufficient information for the investigator to come to a decision. Each investigator should be guided on how to express the outputs of AI systems in a consistent way.

Associated requirement(s):

- All AI systems (including systems that label events and objects) must provide information on the probability of errors (e.g., false positives, false negatives) and other weaknesses (e.g., poorer performance on particular groups) in the model outputs to inform LEA decision making.
- All AI systems should provide direction to LEA investigators on how their output should be expressed in future case communications.
    - Design teams to consider the weight of evidence approach, e.g., weak, inconclusive, strong etc.
- Design teams to consider feasibility of 'masking' certain features in AI system outputs to assist LEAs with understanding the impact of different factors/features on these outputs.
- Design teams to consider whether AI system outputs can be communicated to LEAs through a harmonised approach, without affecting accuracy of information communicated.

- In addition to explainable AI outputs, the INSPECTr Platform and Tools to include an embedded 'Help' section providing in-depth documentation to LEAs aimed towards facilitating understanding outside of any training requirements.

The blockchain technology logs all investigator actions within the INSPECTr Platform and Tools. Developers should consider how appropriate 3rd parties (judges, defence lawyers, etc) could access, query or visualise the logged investigator actions.

Associated requirement(s):

- The blockchain log should be in a format accessible (i.e., understandable) to the relevant range of criminal justice professionals.

4.6 Accountability

Accountability within the INSPECTr Platform and Tools will be partly facilitated by the use of blockchain technology which logs all Platform actions in an immutable manner. In addition, the project ensures regular evaluation of the Platform and Tools in their development phases. INSPECTr includes a variety of AI systems in the Platform and Tools which must be explainable to the investigator. To assist in this achievement, the project evaluation process should consider a harmonised evaluation framework, especially concerning INSPECTr's AI systems.

Associated requirement(s):

- A harmonised project-based (as opposed to partner based) human evaluation process to be considered for all AI systems within design development.
    - The human evaluation process to consider performance and understandability.

5 INSPECTr Ethical, Legal and Social Requirements to Accompany D1.2.0 Functional Requirements

Due to the time between the original submission, and revision, of this deliverable, some updates to the below requirements can be provided. As the implementation of these requirements is still ongoing, it is not appropriate to provide details which could change quickly as this will be outdated rapidly. However, some general information is provided covering initial implementation across the project and tools.

Table 2: INSPECTr Ethics Requirements (January 2021)

#	Requirement Specification	Measurement
1	Platform and Tools: Consider an initial pop-out whereby LEA agrees to lawful basis for use.	Pop-out(s) requiring confirmation of legal basis before the investigator can use an INSPECTr tool exists.
	Having an end-user agree to lawful use of the tools every time they use them could become cumbersome and ineffective. LEAs would need to agree to lawful use of the tools upon receipt of them. Specific operational use would be at the discretion of the LEAs themselves.	
2	Rules engine should be accompanied by clear guidance on its limitations, concerning the varied nature of legal systems, the evolving nature of law, including case law.	Information on rules engine limitations embedded into technology.
	This will be covered in training materials.	
3	All INSPECTr analysers are disabled by default and are individually enabled by LEA senior personnel.	Analysers disabled on first LEA use.
	This is expected to happen, with individual tools enabled by individual LEAs.	
4	Each INSPECTr analyser to be accompanied by detailed information on its functionality allowing senior LEA personnel to decide on the appropriateness of each release.	Clear information pack setting out individual analysers, their benefits and risks to accompany Platform and Tool.
	This will be incorporated into the training materials, and there will be a description of each tool provided in cortex within each docker.	
5	All INSPECTr web-based analysers to be accompanied by a traffic light protocol to identify the security level for the data accessed, e.g., TLP:AMBER.	Analysers that access the web include security level classification via 'Traffic Light Protocol'.
	As noted above, a TLP is planned to be implemented across the platform rather than just for web analysers	

6	Web Scraper Tool to encrypt collected data. • Developers and LEAs to consider which investigators and how investigators decrypt data with a view to ensuring data minimisation.	Web scraper data automatically encrypted.
	Decisions on how data should be treated are expected to be made by the end-user. As such, data is unlikely to be encrypted automatically. However, data segregation would mean that the officer actually engaging in scraping would be the only person able to view that data unless they choose to specifically share it with another.	
7	Web Scraper Tool include filter functionality to provide for limited data gathering where appropriate. • Web scraper design team to consult LEAs on common judicial preferences on filtering to reflect the legal concept of proportionality and to reflect this in so far as is possible in the technical composition.	Web scraper includes personal data filtering functions.
	Filters could be implemented to limit data collection where needed.	
8	Web Scraper Tool design team to consider how the project can avoid unintentional gathering of personal data using filters when the data is located at unusual positions/points on webpage.	Additional web scraper personal data filtering function to be added to capture this requirement.
	Filters are available to prevent excessive data collection.	
9	Computer Vision Tool functionality to be limited to data stored on the INSPECTr Platform.	Computer Vision Tools only compatible with data stored on INSPECTr as LEA evidence.
	The computer vision tools can only be used with data inside of the INSPECTr platform. There is no plan to facilitate INSPECTr access to live data (e.g., real-time CCTV images).	
10	Suspect and Criminal Profiling Tool to be limited to data stored on the INSPECTr Platform.	Suspect and Criminal Profiling Tool only compatible with data stored on INSPECTr as LEA evidence.
	As above.	
11	LEAs should be able to delete their data across the INSPECTr Platform and Tools with relative ease. This means that developers should ensure that data residue is avoided on the Platform and in Tools.	LEA able to delete their INSPECTr data across the Platform in a limited number of steps.

	This function is still in development as the details of the Storage Element Service (SES) and Case Management System are not yet finalised. However, almost all data can be cleaned by the SES, with part-filled (i.e., failed) attempts to write data cleaned during the writing process. Metadata is stored on blockchain and kept in log files.	
12	The design team in consultation with LEAs should consider the automated deletion of data, with prompts alerting LEAs to proactively continue storage. • This is advised especially for INSPECTr network data that has been obscured, such as 'queries' between Member State LEAs.	Automated deletion time frames established, requiring investigator to proactively choose continued storage.
	All data that can be deleted manually can also be deleted automatically via a 'cron-job' (i.e., a chronologically timed action). Data could be flagged for keeping longer and not be subject to a cron-job; for example, an alert could be made a week before a cron-job is due to activate.	
13	All AI systems must seek to adjust existing models for bias to the full extent feasible, e.g., available adjustment data.	Design team to communicate known bias in datasets to LEAs and to identify adjustments made.
	Generally, the models to be provided to LEAs will include information on biases with adjustment measures taken depending on the biases. Where possible, newer models will be provided, and for some tools LEAs will be able to re-train them if biases are found (e.g. the Toolbox: Cross-correlation tool). Other bias mitigation work that requires a proof of concept work could be included in T4.5.4.	
14	All AI systems must display possible bias or reporting issues, according to relative weights in the model, alongside the results of analysis. • Design teams to consider Bayesian or other related approaches for dealing with bias.	Only AI models that account for uncertainty in data used by design team.
	Confidence levels will be reports, and information on residual biases will be discussed in the tool documentation and will be covered in the training materials.	
15	Selection of technical solutions, or decisions about technical features, must take into account how bias may emerge during operational use and the real-world impacts that might arise from this.	INSPECTr partners document possible real-world implications across all AI tools.
	LEA IT staff and operational officers would need to know about biases prior to installing and using the tools. As noted above, documentation and training materials will provide information on biases and how they could impact on LEA use of the tools.	
16	Representation of minority and marginalised groups is an evaluation criterion for participation in testing and capacity building workshops. This includes, but is not	For otherwise equal candidates, persons from minority or marginalised groups should be preferred in the selection of participants in workshops and webinars.

	limited to: sex; gender; ethnicity; socio-economic background; disability, and; physical appearance.	
	Where LEAs and stakeholders are invited to workshops and events, INSPECTr partners will make specific efforts to recruit marginalised persons. For example, asking LEAs to specifically distribute event invitations to, for example, women's or LGBT groups in their organisations.	
17	All AI systems (including systems labelling events and objects) must provide information on errors (e.g., false positives, false negatives) and other weaknesses (e.g., poorer performance on particular groups) in the model outputs to inform LEA decision making.	AI outputs accompanied by clear explanations on their limitations.
	Relevant information will be provided in manuals and training materials.	
18	All AI systems should provide direction to LEA investigators on how the output should be expressed in future case communications. • Design teams to consider the weight of evidence approach, e.g., weak, inconclusive, strong etc.	AI outputs accompanied by directions on how to communicate results in case file and to other criminal justice professionals.
	Tools will provide confidences as results, rather than a definitive answers or decisions. This is because evidence will likely be transferred into the INSPECTr platform without provenance, and so it would be difficult for the tools to be able to dictate how results should be expressed.	
19	Design teams to consider feasibility of 'masking' certain features in AI system outputs to assist LEAs with understanding the impact of different factors/features in the AI output.	AI outputs based on composite information to provide LEAs the capacity to remove individual factors so as to observe impact.
	Partners who are building tools from scratch (e.g., the Toolbox: natural language processing, and the Toolbox: image processing), there should be a function to allow comparison between documents that have been processed by the tool and the original documents. With other tools (e.g., the Toolbox: Cross-correlation, and Toolbox: Crime prediction), information on how the different AI features work will be provided in the documentation. For tools that are not built from scratch, it would not be possible to switch off layers in a neural network, for example, and nor would retraining be expected to provide a sufficient level of control, therefore information could also be provided in the documentation.	
20	Design teams to consider whether AI system outputs can be communicated to LEAs through a harmonised approach, without affecting accuracy of information communicated.	Various AI outputs communicated in harmonised way (to extent possible).

	At this stage, provision of results separately is favoured. However, this will be evaluated after demonstrations have been provided.	
21	In addition to explainable AI outputs, the INSPECTr Platform and Tools to include embedded 'Help' section providing fuller explanations to LEAs aimed towards facilitating understanding outside of any training requirements.	Synthesised INSPECTr training materials to be embedded in 'Help' sections of INSPECTr Platform.
	This information could be provided in the training materials, with links to the training materials provided in the platform itself.	
22	A harmonised (project, as opposed to partner based) human evaluation process to be considered for all AI systems within design development. • The human evaluation process to consider performance and understandability.	INSPECTr partner identified to lead evaluation process across all AI tools.
	It is expected that results should be provided with the data that caused them so the results can be better understood by the end-users, and thereby generate trust in the quality of the model after several months of use.	

In D8.7 Privacy and Ethics-by-Design in the INSPECTr Platform, three additional requirements were added. These are discussed below.

#	Requirement Specification	Measurement
23	If they are more understandable, tools could present results confidences rather than a definitive answer to provide a more accurate picture to end-users.	N/A
	As with requirement 18, tools will provide confidences rather than a definitive answer.	
24	Training materials need to give end-users an adequate understanding of the tools, and so it is essential that it is communicated and understood what the tools can do, what the tools are intended for, and what the tools cannot do.	N/A
	This will be incorporated into training materials guidance on training material content, including these requirements has been provided to technical partners.	
25	Project tools must facilitate categorisation of categories of data-subject (e.g., suspect, criminal, victim, witness, etc.).	N/A

Tags and descriptions related to evidence in the Case Management System (The Hive) can be updated to include these categories.

6 Conclusions

This deliverable set out the main ethical, legal and social issues associated with the INSPECTr Platform and Tools in operational use. It specifies a set of Ethics Requirements, including progress updates made at the revision stage.